

Versione 2.7.0.0

*Technical Support Appliance
Guida alla configurazione*



Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, consultare le informazioni in [“Note legali”](#) a pagina 147.

Ventitreesima edizione (agosto 2020)

Questa edizione si applica alla versione 2, release 7, modifica 0 di IBM® Technical Support Appliance e a tutte le seguenti release e modifiche, a meno che diversamente indicato nelle nuove edizioni.

© **Copyright International Business Machines Corporation 2011, 2020.**

Indice

Figure.....	vii
Capitolo 1. Introduzione.....	1
Account utente e gruppi di utenti.....	1
Ambiti di rilevamento e Serie di ambiti.....	1
Credenziali di rilevamento.....	2
Pianificazione rilevamento.....	2
Pianificazione trasmissione.....	3
Capitolo 2. Prerequisiti.....	5
Scaricare l'immagine TSA.....	5
Requisiti per TSA.....	5
Browser web richiesti.....	5
Requisiti di configurazione per le connessioni al Supporto IBM.....	6
Requisiti di software e credenziale per l'ambiente di rilevamento	6
Capitolo 3. Installazione di Technical Support Appliance.....	9
Installazione utilizzando l'interfaccia web di VMware ESXi.....	9
Installazione di TSA su Microsoft Hyper-V.....	12
Modifica della password per <i>tsaur</i> (obbligatorio).....	19
Configurazione dei dettagli di rete.....	19
Capitolo 4. Configurazione di Technical Support Appliance.....	23
Accesso a Technical Support Appliance.....	23
Accettazione dell'Accordo di licenza.....	25
Utilizzo della Procedura guidata di configurazione per la configurazione iniziale.....	27
Configurazione della connettività IBM.....	28
Registrazione di Technical Support Appliance.....	29
Impostazione dell'orologio.....	31
Configurazione della pianificazione della trasmissione.....	33
Aggiornamento di Technical Support Appliance.....	34
Configurazione delle impostazioni di rete.....	35
Configurazione delle impostazioni di rete di base.....	36
Configurazione delle impostazioni di rete avanzate.....	38
Configurazione dei certificati.....	44
Visualizzazione dello stato del certificato del server SSL.....	45
Generazione e scaricamento di una CSR.....	45
Installazione di un certificato personalizzato (utilizzando i firmatari).....	46
Installazione di un certificato personalizzato (metodo alternativo)	47
Ripristino del certificato predefinito.....	48
Pianificazione della ripulitura dei dati di inventario.....	49
Capitolo 5. Configurazione del rilevamento e della trasmissione a IBM.....	51
Ambiti di rilevamento.....	51
Ambiti dinamici HMC.....	51
Ambiti dinamici VMware.....	59
Ambiti di rilevamento generali.....	68
Importazione di una serie di ambiti.....	73
Impostazioni di rilevamento.....	74

Configurazione delle impostazioni di connessione.....	74
Credenziali di rilevamento.....	75
Visualizzazione delle credenziali.....	75
Visualizzazione dei dettagli delle credenziali.....	75
Aggiunta di credenziali.....	76
Modifica delle credenziali.....	79
Eliminazione delle credenziali.....	80
Pianificazione rilevamento.....	80
Visualizzazione della pianificazione di rilevamento.....	81
Aggiunta della pianificazione di rilevamento.....	82
Modifica della pianificazione di rilevamento.....	84
Disabilitazione della pianificazione di rilevamento.....	85
Eliminazione della pianificazione di rilevamento.....	85
Esecuzione del rilevamento.....	85
Esecuzione del rilevamento su ambiti.....	88
Cronologia rilevamento.....	91
Pianificazione trasmissione.....	91
Visualizzazione della pianificazione della trasmissione.....	92
Modifica della pianificazione della trasmissione.....	92
Disabilitazione della pianificazione della trasmissione.....	94
Esecuzione della trasmissione.....	94
Istantanea dei dati.....	95
Visualizzazione del riepilogo dell'inventario.....	97
Debug di problemi di rilevamento.....	98
Stato autenticazione.....	98
Dispositivi sconosciuti.....	99
Capitolo 6. Configurazione di attività amministrative	101
Informazioni sullo stato.....	101
Visualizzazione del log attività.....	101
Visualizzazione dell'archivio ripulitura inventario.....	102
Password.....	103
Modifica della password.....	103
Sicurezza.....	103
Modifica delle impostazioni di timeout sessione.....	103
Modifica della durata della password.....	104
Backup e ripristino.....	104
Aggiornamento.....	106
Abilitazione della manutenzione pianificata.....	108
Registrazione e traccia.....	109
Arresta.....	110
Strumenti.....	112
Strumenti di rete.....	112
Strumenti database.....	113
Documentazione.....	114
Capitolo 7. Come contattare il supporto IBM per il TSA (Technical Support Appliance).....	117
Apertura di un caso su IBM Support Portal.....	117
Creare una richiesta di servizio tramite l'IBM Call Center.....	117
Appendice A. Installazione di TSA utilizzando il client VMware vSphere.....	119
Appendice B. Configurazione di Technical Support Appliance.....	125
Registrazione di Technical Support Appliance.....	125
Configurazione della connettività IBM.....	127
Impostazione dell'orologio.....	129

Configurazione della pianificazione della trasmissione.....	131
Aggiornamento.....	132
Appendice C. Configurazione dei dettagli di rete DHCP.....	135
Appendice D. Account utente e gruppi di utenti.....	137
Visualizzazione di account utente e gruppi di utenti.....	137
Aggiunta di account utente e gruppi di utenti.....	137
Aggiunta di un gruppo di utenti.....	138
Aggiunta di un account utente.....	140
Modifica di account utente e gruppi di utenti.....	142
Modifica di account utente.....	142
Modifica di gruppi di utenti.....	143
Eliminazione di account utente e gruppi di utenti.....	144
Eliminazione di account utente.....	144
Eliminazione di gruppi di utenti.....	144
Accessibilità.....	145
Note legali.....	147
Marchi.....	148

Figure

1. Crea/Registra VM.....	9
2. Seleziona tipo di creazione.....	10
3. Seleziona file OVF e VMDK.....	10
4. Seleziona storage.....	11
5. Opzioni di distribuzione.....	11
6. Riesaminare la selezione delle impostazioni.....	12
7. Hyper-V Manager.....	13
8. Nome macchina virtuale.....	13
9. Specificare la generazione.....	14
10. Memoria di avvio.....	15
11. Configura rete.....	16
12. Connettere un disco fisso virtuale.....	17
13. Riepilogo.....	18
14. Hyper-V Manager.....	18
15. Modifica password.....	19
16. Nuova password.....	19
17. Impostazione della configurazione di rete.....	19
18. Configurazione di rete.....	20
19. Accedi.....	24
20. Modifica password.....	24
21. Accordo di licenza.....	26
22. Procedura guidata di configurazione.....	27
23. Connettività IBM.....	28

24. Registrazione.....	30
25. Orologio.....	32
26. Per giorno settimanale (dom-sab).....	33
27. Disponibilità degli aggiornamenti.....	34
28. Nessun aggiornamento disponibile.....	35
29. Procedura guidata di configurazione completata.....	35
30. Rete.....	37
31. Accedere alla pagina Rete (avanzate).....	39
32. Rete (avanzate) - Globale.....	40
33. Rete (avanzate) - Interfacce di rete.....	41
34. Rete (avanzate) - Impostazioni DNS.....	42
35. Rete (avanzate) - Route di rete.....	43
36. Nuova route di rete.....	44
37. Stato certificato server SSL.....	45
38. CSR (Certificate Signing Request).....	46
39. Installare il certificato personalizzato.....	47
40. Installazione del certificato personalizzato.....	48
41. Imposta certificato predefinito appliance.....	48
42. Pianificazione pulitura inventario.....	49
43. Ambiti dinamici HMC.....	51
44. Visualizzare una serie di ambiti dinamici HMC.....	52
45. Aggiungere serie di ambiti dinamici HMC.....	54
46. Esempio: Immettere le informazioni di accesso per le LPAR Linux.....	55
47. Ambiti dinamici VMware.....	59
48. Visualizzare una serie di ambiti dinamici VMware.....	60

49. Visualizzare una serie di ambiti dinamici VMware.....	62
50. Immettere le informazioni di accesso per la macchina virtuale Linux.....	63
51. Immettere le informazioni di accesso per la macchina virtuale Windows.....	64
52. Serie di ambiti di rilevamento.....	69
53. Ambiti di rilevamento generali.....	70
54. Importa serie di ambiti.....	74
55. Nuove credenziali di rilevamento.....	75
56. Dettagli credenziali di rilevamento.....	76
57. Nuove credenziali di rilevamento.....	77
58. Pianificazione rilevamento.....	81
59. Aggiungi pianificazione rilevamento.....	83
60. Per giorno settimanale (dom-sab).....	84
61. Eseguire il rilevamento su ambiti specifici.....	86
62. Ambiti dinamici HMC.....	87
63. Eseguire il rilevamento su ambiti dinamici VMWare.....	87
64. Ambiti di rilevamento.....	88
65. Eseguire il rilevamento su ambiti specifici.....	89
66. Ambiti dinamici HMC.....	89
67. Eseguire il rilevamento su ambiti specifici.....	90
68. Ambiti dinamici VMWare.....	90
69. Eseguire il rilevamento su ambiti dinamici VMWare.....	91
70. Cronologia rilevamento.....	91
71. Modifica della pianificazione della trasmissione.....	93
72. Per giorno settimanale (dom-sab).....	93
73. Esegui ora la trasmissione.....	95

74. Istantanea dei dati.....	96
75. Data dell'istantanea dei dati.....	96
76. Riepilogo inventario.....	97
77. Dettagli riepilogo inventario.....	98
78. Stato autenticazione.....	99
79. Log attività.....	101
80. Archivio pulitura inventario.....	102
81. Backup e ripristino.....	105
82. Aggiornamento.....	107
83. Disponibilità degli aggiornamenti.....	107
84. Esegui ora l'aggiornamento.....	108
85. Registrazione e traccia.....	110
86. Arresta.....	111
87. Strumenti di rete.....	112
88. Documentazione.....	115
89. Distribuzione del modello OVF.....	119
90. Origine del modello OVF.....	120
91. Nome e ubicazione.....	121
92. Storage.....	122
93. Formato disco.....	123
94. Pronto al completamento.....	124
95. Registrazione.....	126
96. Connettività IBM.....	128
97. Orologio.....	130
98. Modifica della pianificazione della trasmissione.....	131

99. Per giorno settimanale (dom-sab).....	132
100. Aggiornamento.....	133
101. Disponibilità degli aggiornamenti.....	133
102. Esegui ora l'aggiornamento.....	134
103. Impostazione della configurazione di rete.....	135
104. Configurazione di rete.....	135
105. Indirizzo IP DHCP.....	136
106. Gruppi.....	138
107. Aggiungi gruppo di utenti.....	139
108. Account utente e gruppi.....	140
109. Aggiungi account utente.....	141
110. Modificare l'account utente admin.....	143

Capitolo 1. Introduzione

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 le applicazioni, il middleware, i server e i componenti di rete nel data center.

TSA include un'interfaccia utente basata sul web per configurare e personalizzare l'accesso al sistema e ai dati. L'interfaccia utente permette di modificare le pianificazioni per il rilevamento e la trasmissione dei dati.

Come parte del processo di rilevamento, TSA inizialmente tenta di rilevare gli endpoint nell'ambito definito, senza utilizzare credenziali di rilevamento. Questo implica l'utilizzo di Nmap e tenta di rilevare e classificare i dispositivi con scansione IP minima, creazione di impronta digitale dello stack e associazione porta. In genere, questa attività non è tanto significativa da disattivare un IDS (intrusion detection system), ma potrebbe essere necessario in caso di rigide impostazioni locali.

La 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.

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.

Account utente e gruppi di utenti

L'esecuzione di qualsiasi funzione di TSA richiede un certo livello di autorizzazione. Se un utente autenticato tenta di eseguire una funzione senza il livello di autorizzazione appropriato, viene visualizzato un errore e la funzione non viene eseguita.

In un'organizzazione, è possibile creare ruoli per varie funzioni lavoro. Le autorizzazioni a eseguire certe operazioni sono assegnate a ruoli specifici. Agli utenti TSA sono assegnati specifici ruoli, e tramite tali assegnazioni di ruoli hanno le autorizzazioni necessarie per eseguire particolari funzioni di sistema. In questo modo, tutti gli utenti a cui è assegnato un ruolo avranno livelli di autorizzazione associati al ruolo ed è semplice aggiungere un utente a un ruolo, modificare il ruolo degli utenti o rimuoverlo.

In TSA, i ruoli sono gestiti con gruppi di utenti che hanno livelli di autorizzazione associati. Gli utenti sono gestiti con account utente. Agli account utente può essere assegnata l'appartenenza a uno o più gruppi di utenti e, tramite tali appartenenze, gli utenti hanno il livello di autorizzazione per eseguire funzioni particolari.

Inoltre, i gruppi di utenti possono essere ulteriormente limitati a serie di ambiti selezionate. Una serie di ambiti è una raccolta di indirizzi IP, intervalli di indirizzi o subnet che identificano gli elementi IT che TSA può rilevare. Specificare limitazioni di serie di ambiti per un gruppo di utenti è un modo per limitare ulteriormente l'accesso dei membri di tale gruppo di utenti. Ad esempio, è possibile creare gruppi di utenti specifici della piattaforma, ad esempio utenti responsabili per la manutenzione dei sistemi Linux®, tramite una combinazione di livello di autorizzazione e limitazioni di serie di ambiti associati a un particolare gruppo di utenti.

Ambiti di rilevamento e Serie di ambiti

Gli ambiti di rilevamento identificano le risorse che si desidera che TSA rilevi. Gli ambiti di rilevamento sono raggruppati in serie di ambiti di rilevamento.

È possibile specificare gli ambiti di rilevamento utilizzando un indirizzo IP, un intervallo di indirizzi IP o una rete o subnet per definire le risorse cui si accede durante il rilevamento. Un ambito di rilevamento può essere piccolo quanto un solo indirizzo IP o grande quanto un intervallo di indirizzi IP o una rete.

Per semplificare la creazione di una serie di ambiti, è possibile utilizzare un file per importare un elenco di indirizzi IP. Per maggiori informazioni, consultare la sezione [“Importazione di una serie di ambiti”](#) a pagina 73.

Più indirizzi IP ci sono nell'ambito di rilevamento e più tempo impiega il rilevamento. È possibile modificare la dimensione del rilevamento disabilitando o abilitando le serie di ambiti di rilevamento o escludendo indirizzi IP, intervalli di indirizzi IP, reti o subnet da un ambito in una serie di ambiti.

Nota: Per prestazioni ottimali, limitare il numero cumulativo di indirizzi IP (indirizzi IP, intervalli, subnet e esclusioni) in una serie di ambiti a un massimo di 400.

Attività correlate

[Aggiunta di account utente e gruppi di utenti](#)

È possibile aggiungere account utente e gruppi di utenti per controllare l'accesso alle funzioni di TSA.

Credenziali di rilevamento

Le credenziali di rilevamento sono una raccolta di nomi utente, password o chiavi SSH e stringhe di community SNMP (Simple Network Management Protocol) utilizzate da TSA per accedere alle risorse durante il rilevamento.

È necessario configurare e gestire le credenziali di rilevamento per le risorse che si desidera rilevare. Le informazioni di accesso da fornire variano in base al tipo di credenziale, ma generalmente includono almeno il nome utente e la password o la chiave SSH.

Una credenziale di rilevamento può essere applicata a tutte le serie di ambiti o limitata a una singola serie di ambiti. Se si definiscono credenziali che si applicano a una singola serie di ambiti si migliorano le prestazioni e si evitano tentativi di accesso non validi, che possono portare al blocco dell'account.

Quando si accede a una risorsa, il TSA utilizza in sequenza ogni credenziale associata a un particolare ambito nell'ordine di elencazione della pagina **Credenziali di rilevamento** finché la risorsa non concede a TSA l'autorizzazione ad accedervi. Ad esempio, quando si accede a un computer, il TSA utilizza il primo nome utente e password specificati nell'elenco di credenziali per i computer e associati alla serie di ambiti che li contiene. Se il nome utente e la password non sono corretti per uno specifico computer, il TSA utilizza automaticamente i successivi nome utente e password specificati nell'elenco di credenziali per i computer.

Suggerimento: Prima di salvare le credenziali, è possibile verificare se sono state specificate credenziali valide per i tipi di sistema, ad esempio **Computer**, **Computer (Windows)**, **SNMP** o **SNMPV3**. Con questo test ci si assicura che le credenziali siano definite in modo valido.

Suggerimento:

- Utilizzare un account di servizio con una password comune per tutti i dispositivi di un determinato tipo, ad esempio AIX o Windows. Quindi, è possibile definire una singola credenziale per rilevare tutte le istanze di questo tipo di dispositivo.
- Utilizzare account con password che non scadono.
- Utilizzare chiavi SSH, dove necessario.

Pianificazione rilevamento

I rilevamenti sono eseguiti su giorni e ore pianificati per garantire che i dati rilevati siano sempre attuali e accurati. TSA prevede una pianificazione "Rilevamento completo" predefinita per il rilevamento di tutte le serie di ambiti definite. Tale pianificazione predefinita potrà essere modificata in base alle proprie esigenze. È possibile, inoltre, creare pianificazioni che consentano di estendere il rilevamento di serie di

ambiti a ore e date differenti. È anche possibile visualizzare i dettagli, la cronologia e lo stato dell'ultimo rilevamento eseguito.

Quando si modifica una pianificazione del rilevamento, specificare il nome, le serie di ambiti, l'ora di inizio e la frequenza dei rilevamenti. Se la pianificazione del rilevamento è il rilevamento predefinito, è possibile modificare solo l'ora di inizio e la frequenza dei rilevamenti. È anche possibile eseguire rilevamenti su richiesta.

La durata del rilevamento varia in base a un numero di fattori, tra cui il numero e la complessità delle risorse, e può richiedere fino a 72 ore per il completamento.

Pianificazione trasmissione

I dati rilevati vengono impacchettati e trasmessi in modo sicuro al supporto IBM nei giorni e orari pianificati per garantire che IBM abbiano le informazioni più attuali e accurate. TSA ha una pianificazione di trasmissione predefinita che è possibile modificare in base alle esigenze. È anche possibile eseguire trasmissioni su richiesta. È anche possibile visualizzare lo stato dell'ultima trasmissione eseguita.

Il tempo impiegato per una trasmissione varia in base alla quantità di dati rilevati.

Capitolo 2. Prerequisiti

Per configurare e utilizzare TSA, è necessario assicurarsi di soddisfare determinati prerequisiti, come le credenziali richieste per l'ambiente di rilevamento e requisiti di configurazione per la connessione al supporto IBM.

Nota: Tutti i prerequisiti nelle seguenti sezioni sono obbligatori per TSA tranne i requisiti specificati nella sezione [“Requisiti per TSA”](#) a pagina 5.

Scaricare l'immagine TSA

Le immagini TSA sono disponibili per entrambi i server Microsoft Hyper-V [*TSA-HYPERV-<versione>*] e VMware [*TSA-VMWARE-<versione>*].

È possibile reperire le istruzioni per lo scaricamento all'indirizzo: <https://ibm.biz/TSAdemo>

Requisiti per TSA

Prima di configurare e utilizzare TSA, assicurarsi di soddisfare i seguenti prerequisiti.

Hardware x86 a 64 bit

TSA deve essere caricato su sistemi x86 a 64 bit.

Hypervisor

TSA richiede VMware ESXi o Microsoft Hyper-V

Nota: È consigliato utilizzare una versione attualmente supportata di ESXi o Hyper-V.

Processore

TSA richiede un processore con almeno 2,26 GHz e quattro core.

CPU

TSA richiede quattro CPU a 64 bit.

Memoria

TSA richiede 16 GB di memoria.

DASD (Direct Access Storage Device)

TSA richiede 150 GB di DASD.

Rete

TSA richiede un adattatore Ethernet da 1 Gigabit.

Browser web richiesti

Per configurare e monitorare il rilevamento e la trasmissione, viene utilizzata un'interfaccia utente basata su web.

TSA supporta i seguenti browser internet:

- Mozilla Firefox V68.9.0 Extended Support Release (ESR)
- Microsoft Edge V83.0.478.54 for Windows 10
- Google Chrome V83.0.4103.116 (64-bit)

È possibile scaricare questi browser dai seguenti siti:

- [Mozilla Firefox](http://www.mozilla.org/products/firefox/) (<http://www.mozilla.org/products/firefox/>)
- [Microsoft Edge](https://www.microsoft.com/en-us/edge) (<https://www.microsoft.com/en-us/edge>)

- [Google Chrome \(https://support.google.com/chrome/answer/95346?hl=en\)](https://support.google.com/chrome/answer/95346?hl=en)

Requisiti di configurazione per le connessioni al Supporto IBM

TSA può connettersi al supporto IBM tramite connessione diretta o tramite un proxy fornito dall'utente che deve essere configurato in modo da consentire la comunicazione con IBM. Se si utilizza un proxy, l'ispezione TLS/SSL non è supportata. Alle richieste tramite un proxy deve essere consentito di fluire direttamente a IBM senza terminazione TLS/SSL.

Assicurarsi che il firewall consenta le connessioni al nome host e agli indirizzi IP del server IBM, come spiegato nella tabella [Connessioni di rete](#). Se la rete non consente l'accesso ai server IBM, le transazioni di TSA al supporto IBM avranno esito negativo.

<i>Tabella 1. Connessioni di rete</i>			
Nome DNS	Indirizzo IP	Porta	Protocollo
esupport.ibm.com	129.42.54.189	443	HTTPS (a IBM)
	129.42.56.189		
	129.42.60.189		

L'ambiente del server IBM è totalmente compatibile con NIST SP800-131A, supporta il protocollo TLS 1.2, SHA-256 o funzioni hash più complesse e chiavi RSA con complessità di almeno 2048 bit.

Nota: L'ispezione SSL non è supportata, se la si utilizza sul proxy, disabilitarla per questi flussi.

Per i proxy Blue Coat, disabilitare il "rilevamento di protocolli" per i server IBM. Aggiungere queste regole di configurazione:

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

Requisiti di software e credenziale per l'ambiente di rilevamento

Per poter effettuare il rilevamento di endpoint o risorse nell'ambiente, TSA deve avere accesso a tali risorse. Si consiglia di creare un account di servizio su ciascuna risorsa che è specificamente per TSA, da utilizzare durante l'accesso a tale risorsa.

Dopo aver creato un account di servizio su una risorsa, è necessario definire e gestire le credenziali su TSA che corrispondono alle credenziali definite sulla risorsa per tale account di servizio. TSA utilizza queste credenziali per accedere alla risorsa. I requisiti per le credenziali variano in base all'ambiente e al tipo di risorsa che si desidera rilevare, ma generalmente includono un nome utente e una password o una chiave SSH. Alcune risorse hanno anche requisiti di software specifici.

Tipo di credenziale	Informazioni di accesso
Computer	<p>Nome utente: Il nome utente per accedere al dispositivo.</p> <p>Password/Passphrase: Password/passphrase per accedere al dispositivo.</p> <p>Tipo di autenticazione: Il tipo di autenticazione per il dispositivo.</p> <ul style="list-style-type: none"> • Password - Utilizzare la password fornita. • PKI - Utilizzare la chiave SSH associata alla serie di ambiti specifica.
Computer (Windows)	<p>Nome utente: Il nome utente per accedere al computer Windows.</p> <p>Password: La password per accedere al computer Windows.</p>
Elemento rete (SNMP)	<p>Stringa community: La stringa community per il dispositivo.</p>
Elemento rete (SNMPV3)	<p>Nome utente: Il nome utente per accedere al dispositivo.</p> <p>Password: La password per accedere al dispositivo.</p> <p>Password privata: La password utilizzata se la codifica dei dati è impostata per SNMP.</p> <p>Protocollo di autenticazione: Il tipo di protocollo di autenticazione utilizzato da SNMP.</p> <ul style="list-style-type: none"> • Nessuno • MD5 • SHA
Altro (dispositivo Cisco)	<p>Nome utente: Il nome utente per accedere al dispositivo Cisco.</p> <p>Password: La password per il dispositivo Cisco.</p> <p>Password di abilitazione: La password di abilitazione per il dispositivo Cisco.</p>
Altro (lavori Cisco)	<p>Nome utente: Il nome utente per accedere al server CiscoWorks.</p> <p>Password: La password per accedere al server CiscoWorks.</p>

Nota: Per ulteriori informazioni sui requisiti di software e credenziali, fare riferimento alla Guida dell'assistente alla configurazione.

Capitolo 3. Installazione di Technical Support Appliance

TSA include software pre-installato. Viene compresso e distribuito come un'immagine per le installazioni VMware o come immagine VHDX per le installazioni Hyper-V Microsoft. Per VMware, TSA può essere installato utilizzando il client VMware vSphere o l'interfaccia web VMware (per ESXi). Per Hyper-V, TSA può essere installato utilizzando Hyper-V Manager. Questa sezione fornisce la procedura per l'installazione di TSA utilizzando uno o l'altro di questi metodi.

Installazione utilizzando l'interfaccia web di VMware ESXi

Prima di iniziare

TSA richiede che sia caricato VMware ESXi 6.5, o versioni successive, per controllare l'hardware.

Informazioni su questa attività

Attenersi alla seguente procedura per installare l'immagine TSA.

Procedura

1. Accedere al sistema ESXi tramite l'interfaccia Web VMware ESXi.
2. Fare clic su **Crea/Registra VM**. Viene visualizzata la procedura guidata **Nuova macchina virtuale**.



Figura 1. Crea/Registra VM

3. Nella schermata **Seleziona tipo di creazione**, selezionare l'opzione **Distribuisce una macchina virtuale da un file OVF o OVA** e fare clic su **Avanti**.

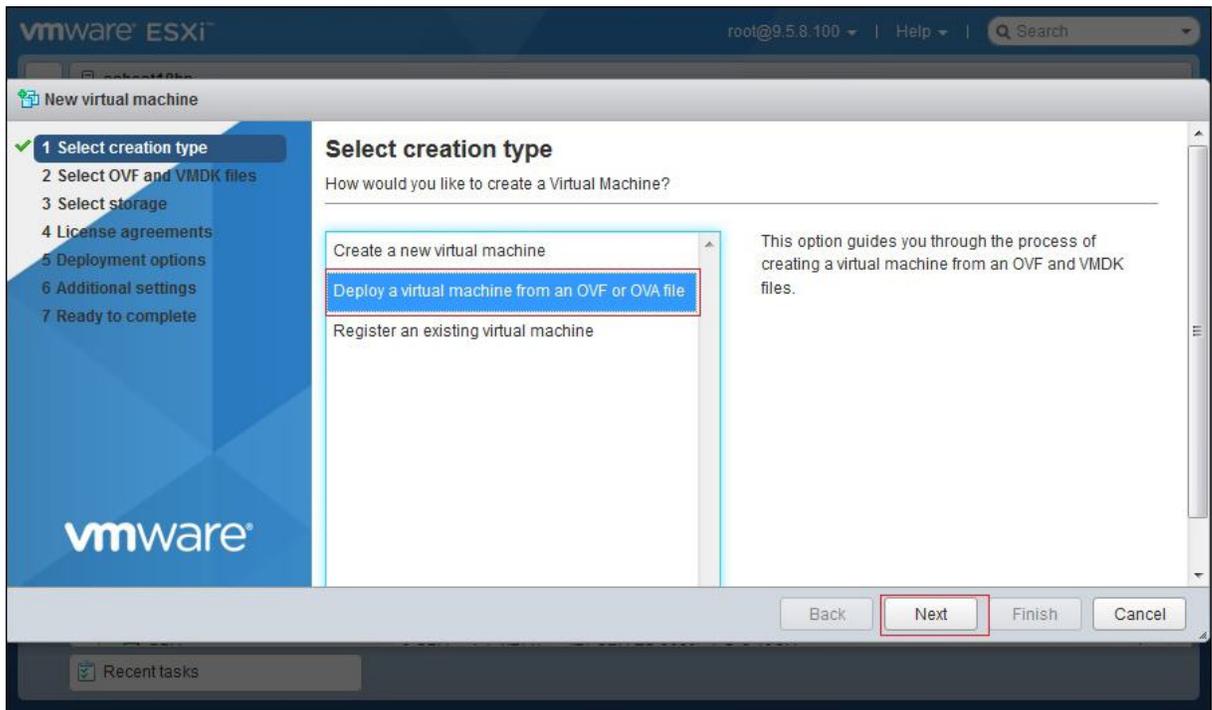


Figura 2. Seleziona tipo di creazione

4. Nella schermata **Seleziona file OVF e VMDK**, immettere un nome per la macchina virtuale oppure è possibile utilizzare il valore predefinito.

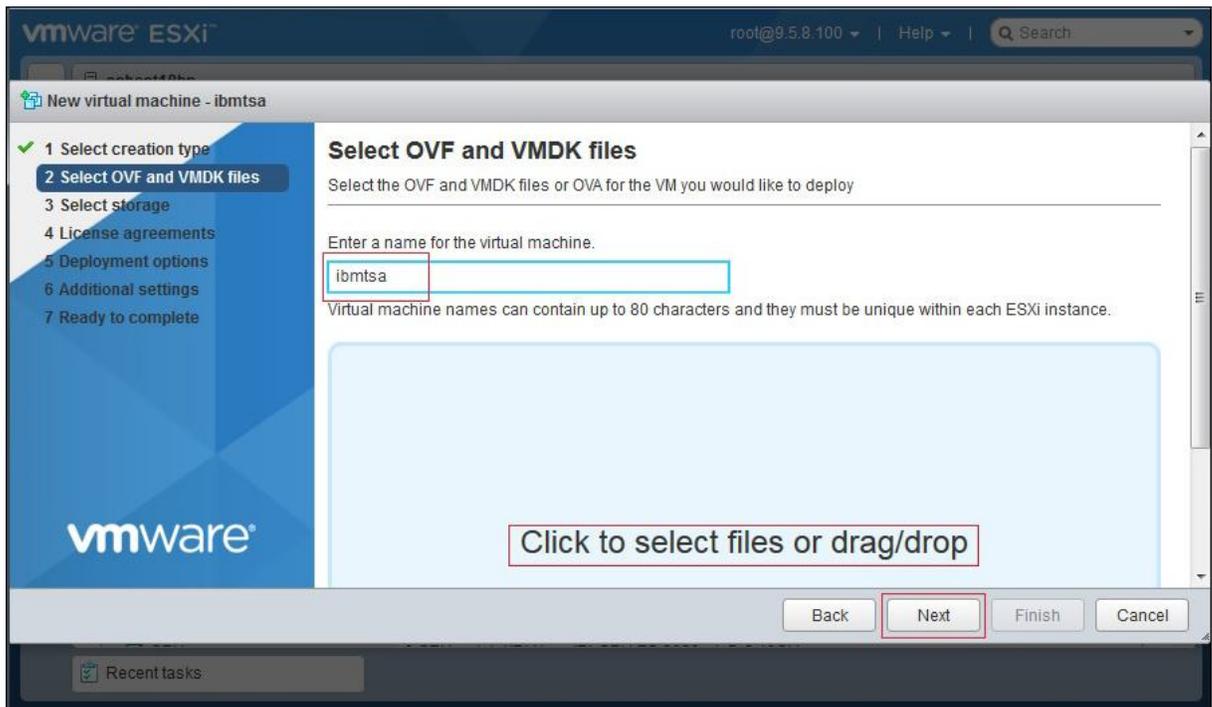


Figura 3. Seleziona file OVF e VMDK

5. Fare clic all'interno della casella **Fare clic per selezionare i file o trascinare la selezione** e selezionare il file immagine scaricato da Fix Central, quindi fare clic su **Avanti**.
6. Nella schermata **Seleziona storage**, dall'elenco visualizzato, selezionare un archivio dati nel quale archiviare la configurazione e i file del disco. Quindi, fare clic su **Avanti**.

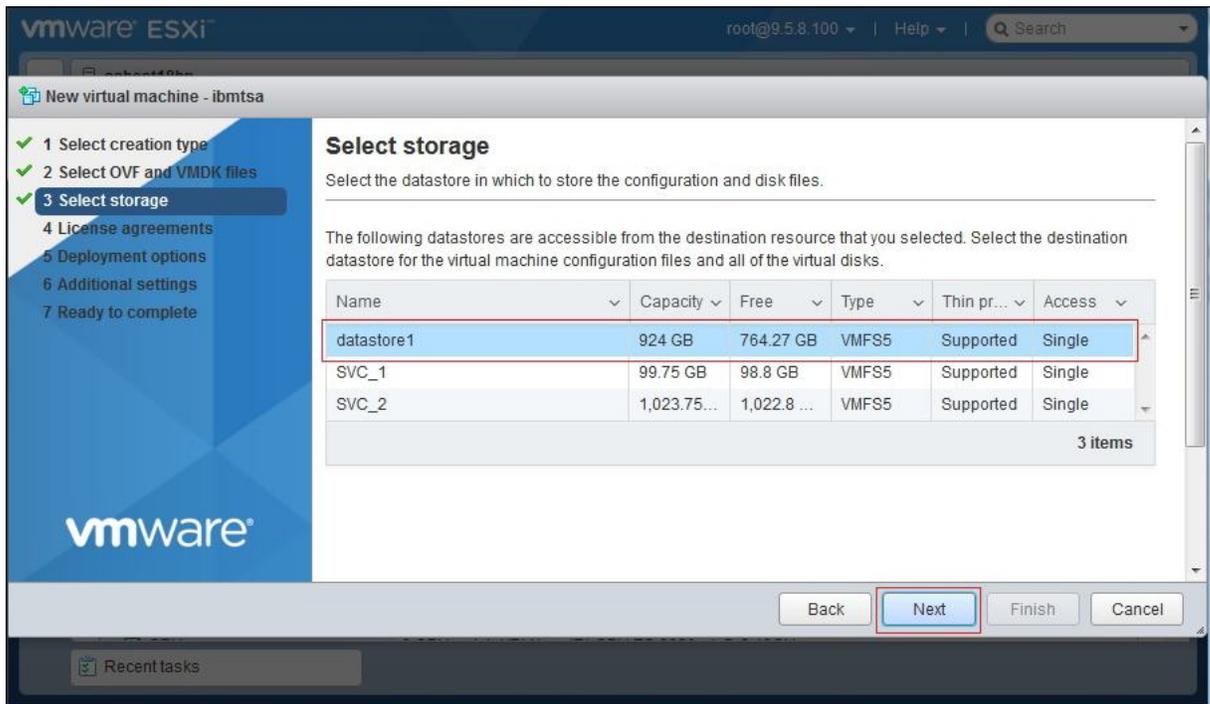


Figura 4. Seleziona storage

7. Nella schermata **Opzioni di distribuzione**, selezionare le associazioni di rete dall'elenco a discesa **Rete VM**.

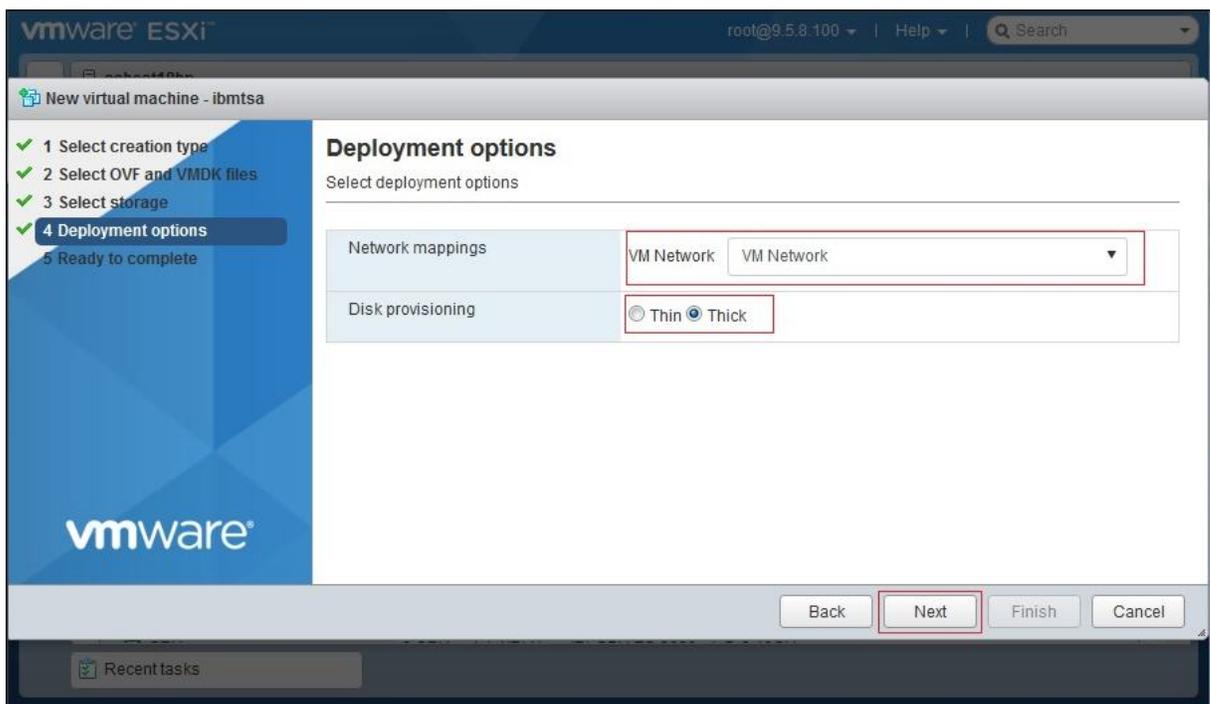


Figura 5. Opzioni di distribuzione

8. Selezionare l'opzione **Thick** per il provisioning del disco, quindi fare clic su **Avanti**.
9. Nella schermata **Pronto al completamento**, rivedere tutte le impostazioni specificate. Se si desidera apportare modifiche, fare clic su **Indietro** ed effettuare modifiche alle opzioni rilevanti. Quando si è soddisfatti, fare clic su **Fine**.

Importante: Non aggiornare il browser durante la distribuzione della macchina virtuale.

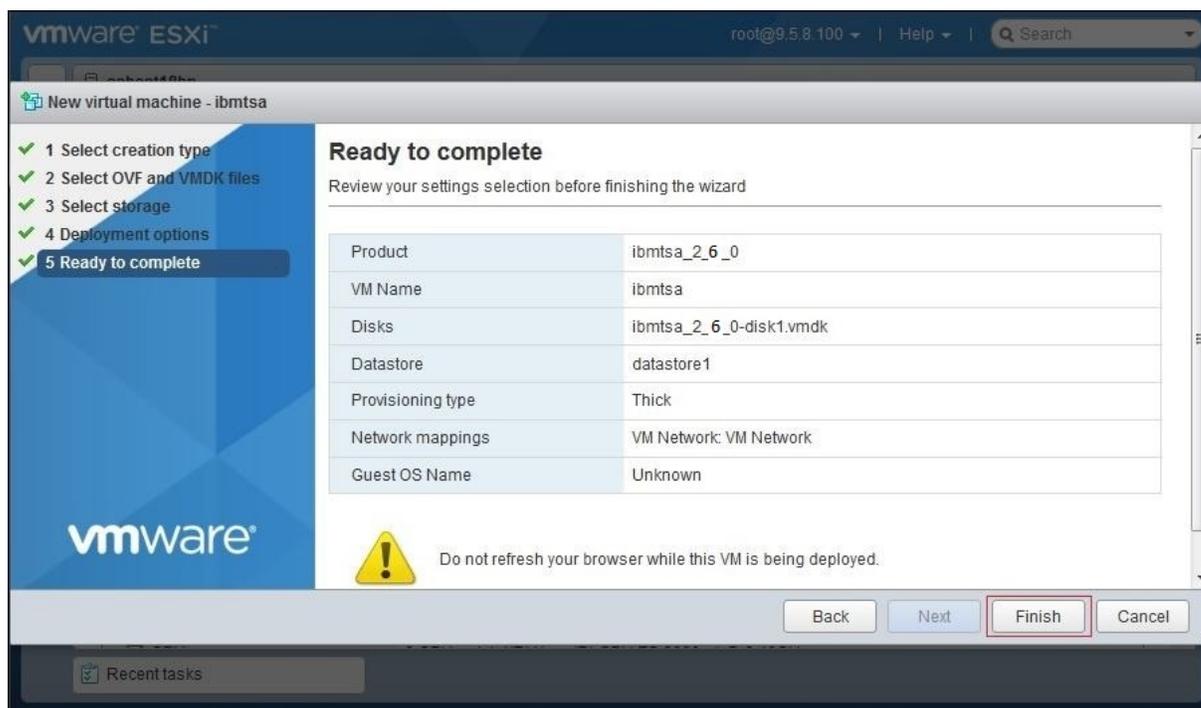


Figura 6. Riesaminare la selezione delle impostazioni

La macchina virtuale di TSA viene installata sul sistema.

10. Nella console di TSA, immettere **ibmtsa login** come **tsaurx** e **Password** come **configTsa**.
11. Richiesto: Per modificare la password di accesso, continuare con i passi elencati nella sezione [“Modifica della password per tsaur \(obbligatorio\)”](#) a pagina 19.
12. Per completare l'installazione, continuare con i passi elencati nella sezione [“Configurazione dei dettagli di rete”](#) a pagina 19.

Installazione di TSA su Microsoft Hyper-V

Prima di iniziare

Prima di configurare e utilizzare TSA su Hyper-V, assicurarsi di soddisfare i seguenti prerequisiti:

- Hyper-V Server 2012, 2016 o 2019
- Hyper-V Manager
- Switch di rete virtuale creato tramite Hyper-V Manager

Informazioni su questa attività

Attenersi alla seguente procedura per installare TSA su Hyper-V.

Procedura

Per installare TSA su Hyper-V, attenersi alla seguente procedura:

1. Dopo aver scaricato l'immagine di TSA, estrarre il file *ibmtsa_2700.vhdx* da *ibmtsa_2700.zip* e spostarlo in una directory su Hyper-V Server.
2. Avviare Hyper-V Manager e stabilire una connessione a Hyper-V Server dal sistema client.
3. Fare clic su **Sfogliare** e selezionare l'immagine salvata sul sistema.

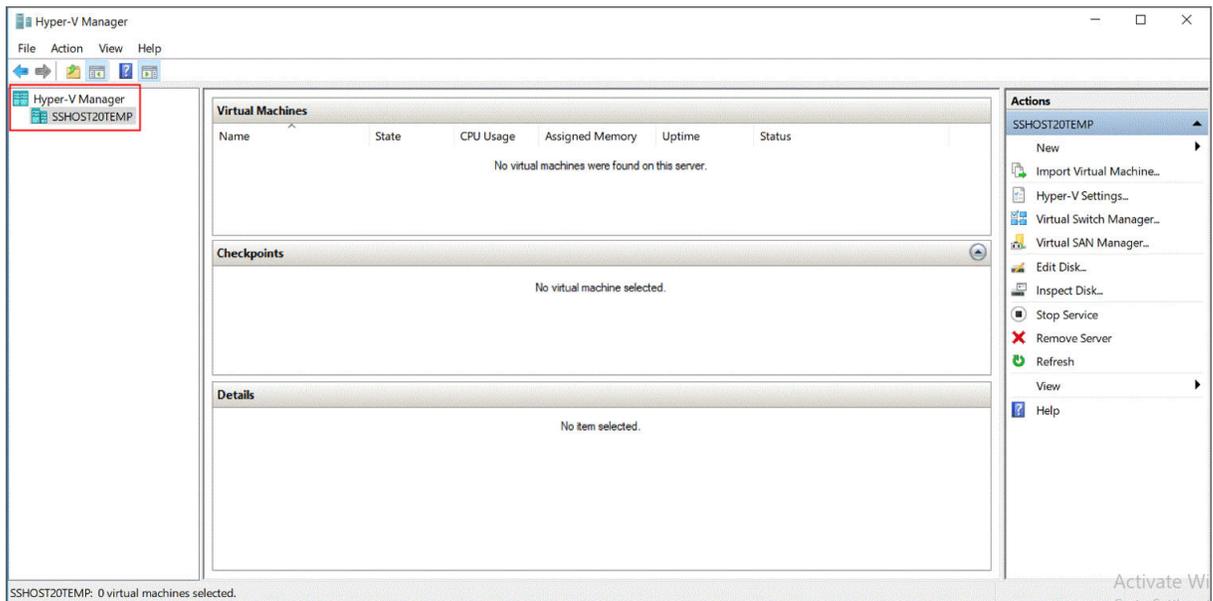


Figura 7. Hyper-V Manager

4. Dal menu **Azioni**, selezionare **Nuovo** → **Macchina virtuale**. Viene visualizzata la **Procedura guidata Nuova macchina virtuale**.
5. Immettere il **Nome** per la nuova macchina virtuale e fare clic su **Avanti**.

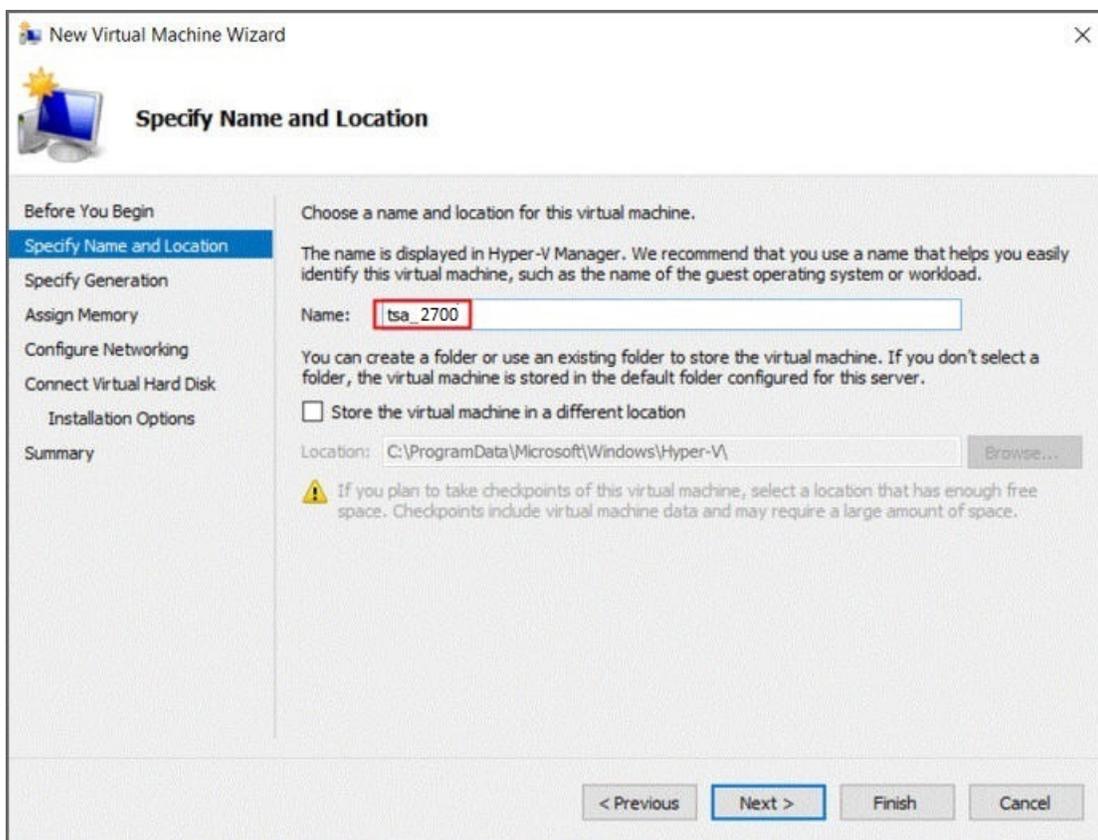


Figura 8. Nome macchina virtuale

6. Selezionare **Generazione 1** come generazione della macchina virtuale e fare clic su **Avanti**.

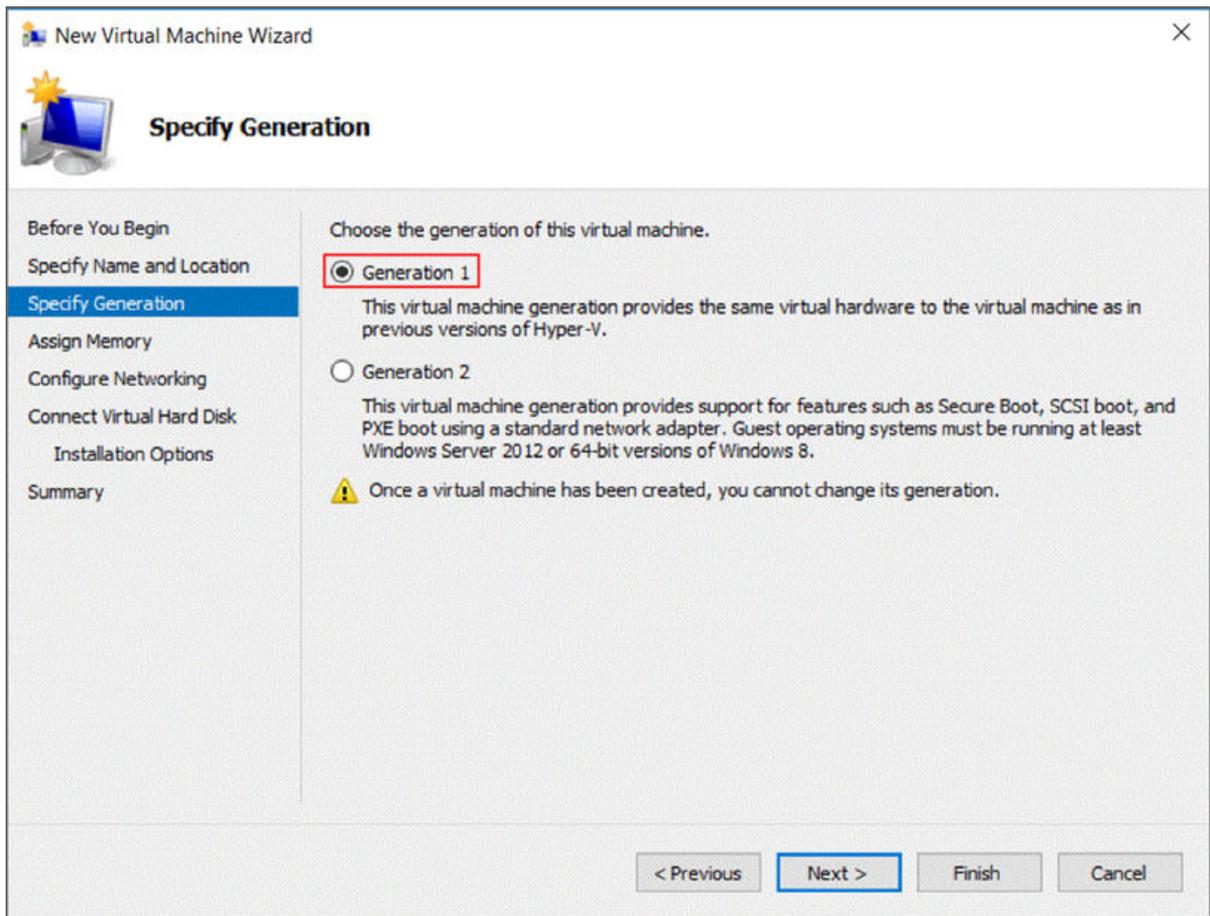


Figura 9. Specificare la generazione

7. Immettere **Memoria di avvio** come 16384 MB e fare clic su **Avanti**.

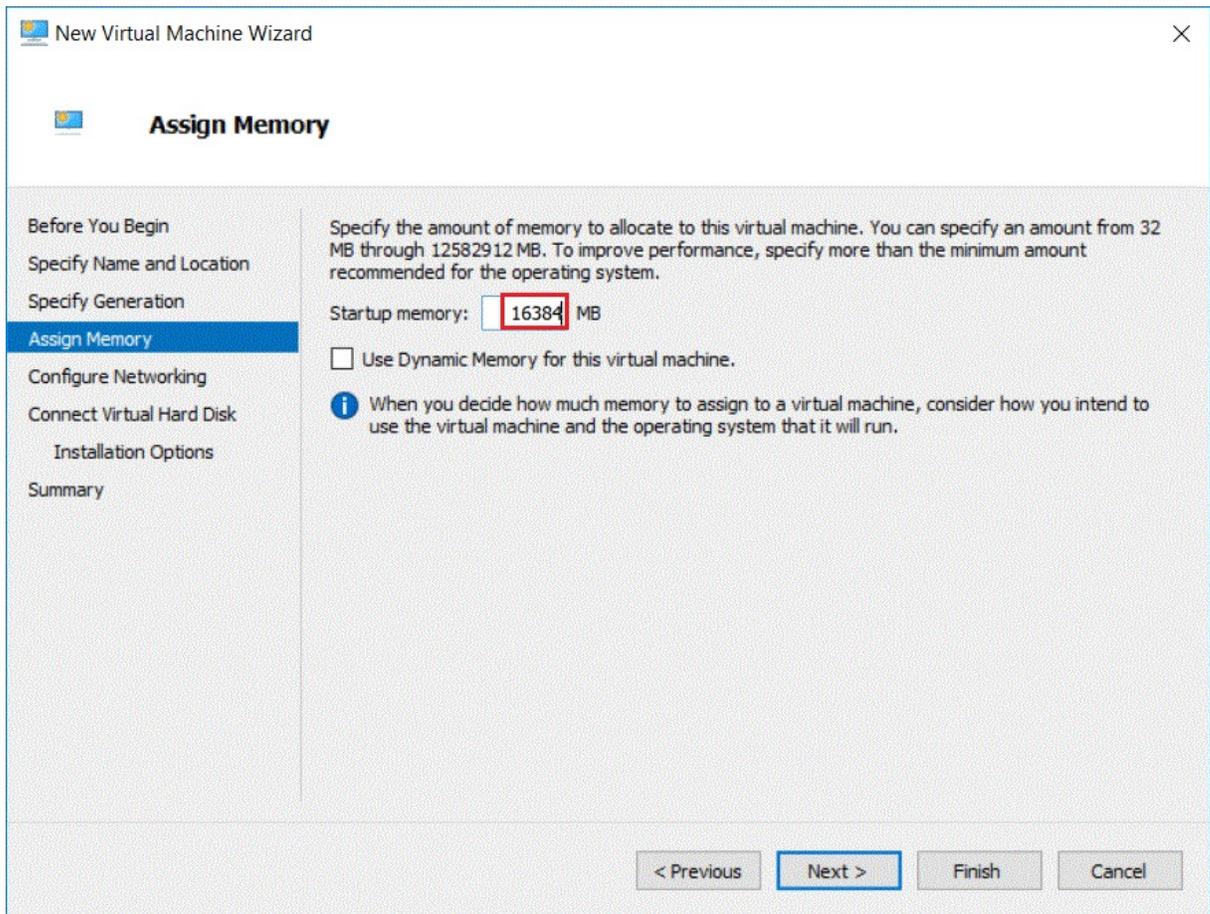


Figura 10. Memoria di avvio

8. Selezionare uno switch virtuale preconfigurato e fare clic su **Avanti**.

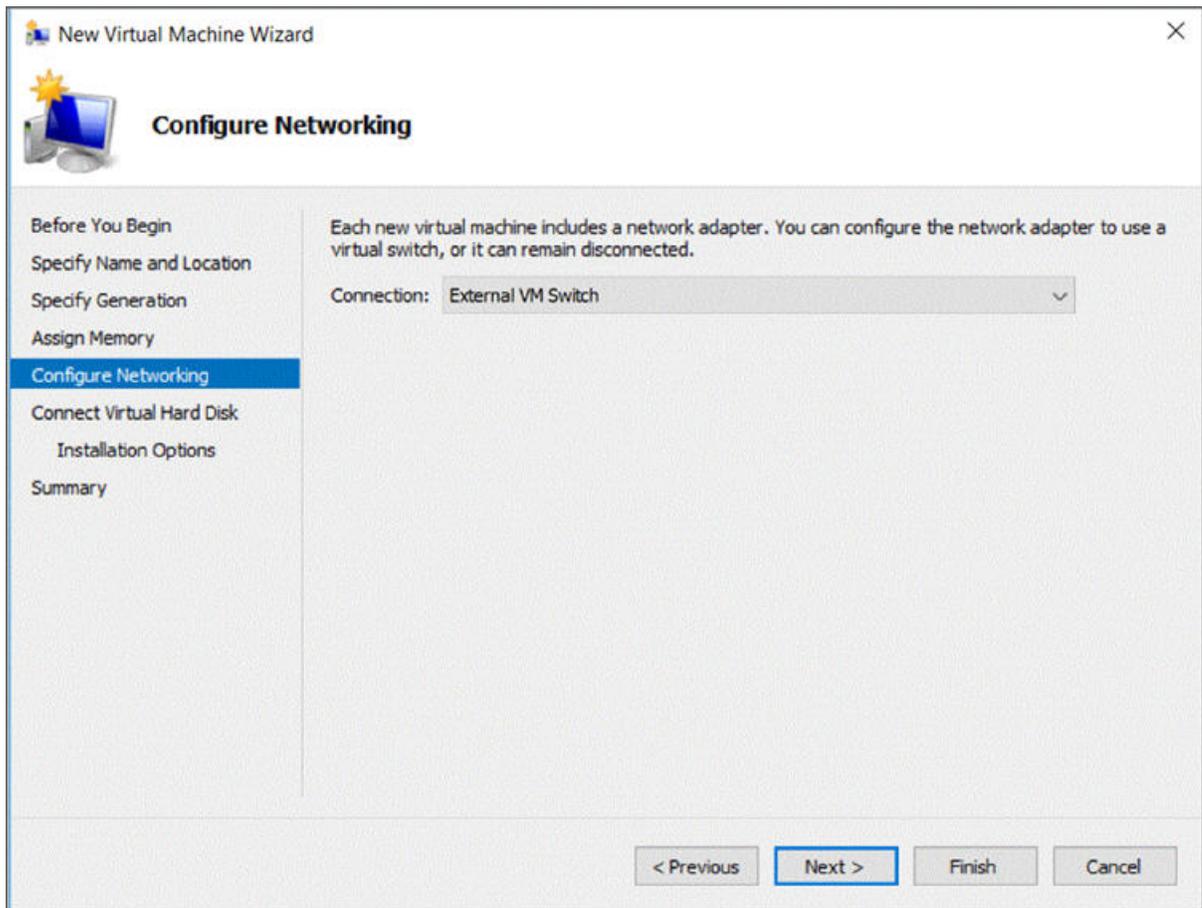


Figura 11. Configura rete

9. Selezionare l'opzione **Usa un disco fisso virtuale esistente** e ricercare il file `ibmtsa_2700.vhdx` copiato su Hyper-V Server nel Passo 2 e fare clic su **Avanti**.

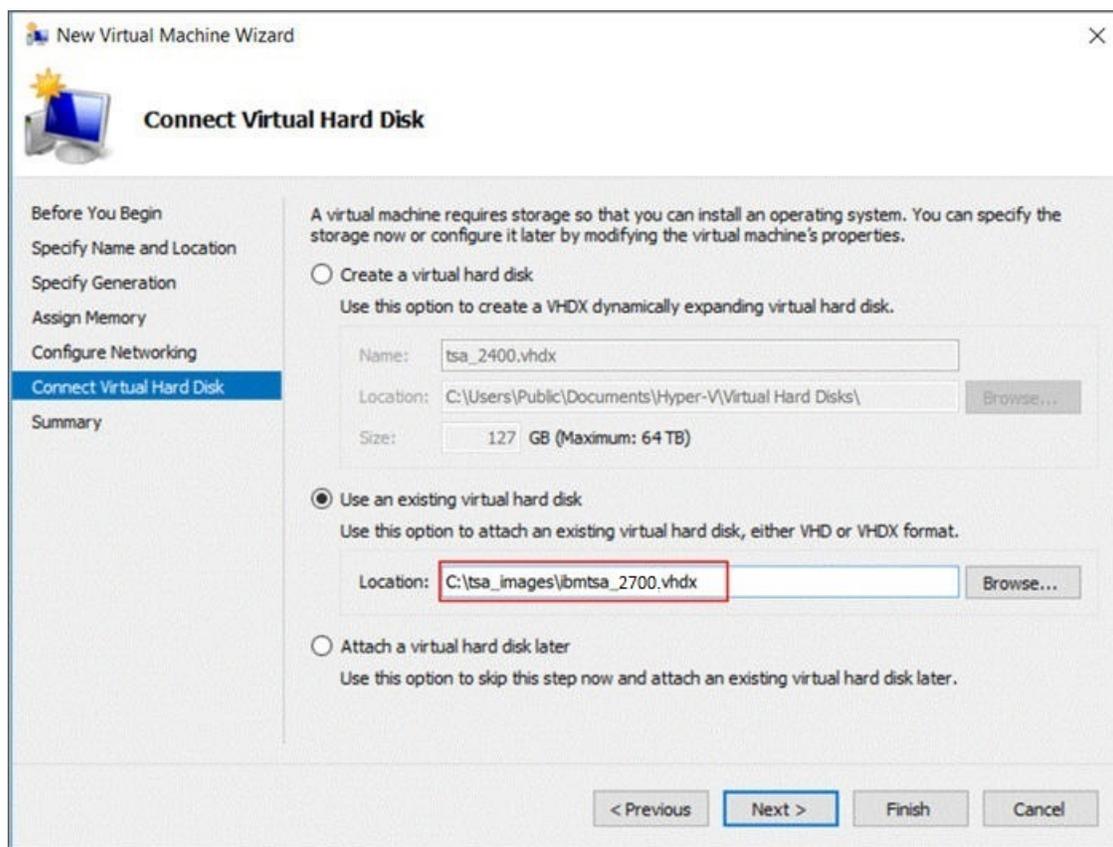


Figura 12. Connettere un disco fisso virtuale

10. Nella pagina **Riepilogo**, rivedere le impostazioni e fare clic su **Fine**.

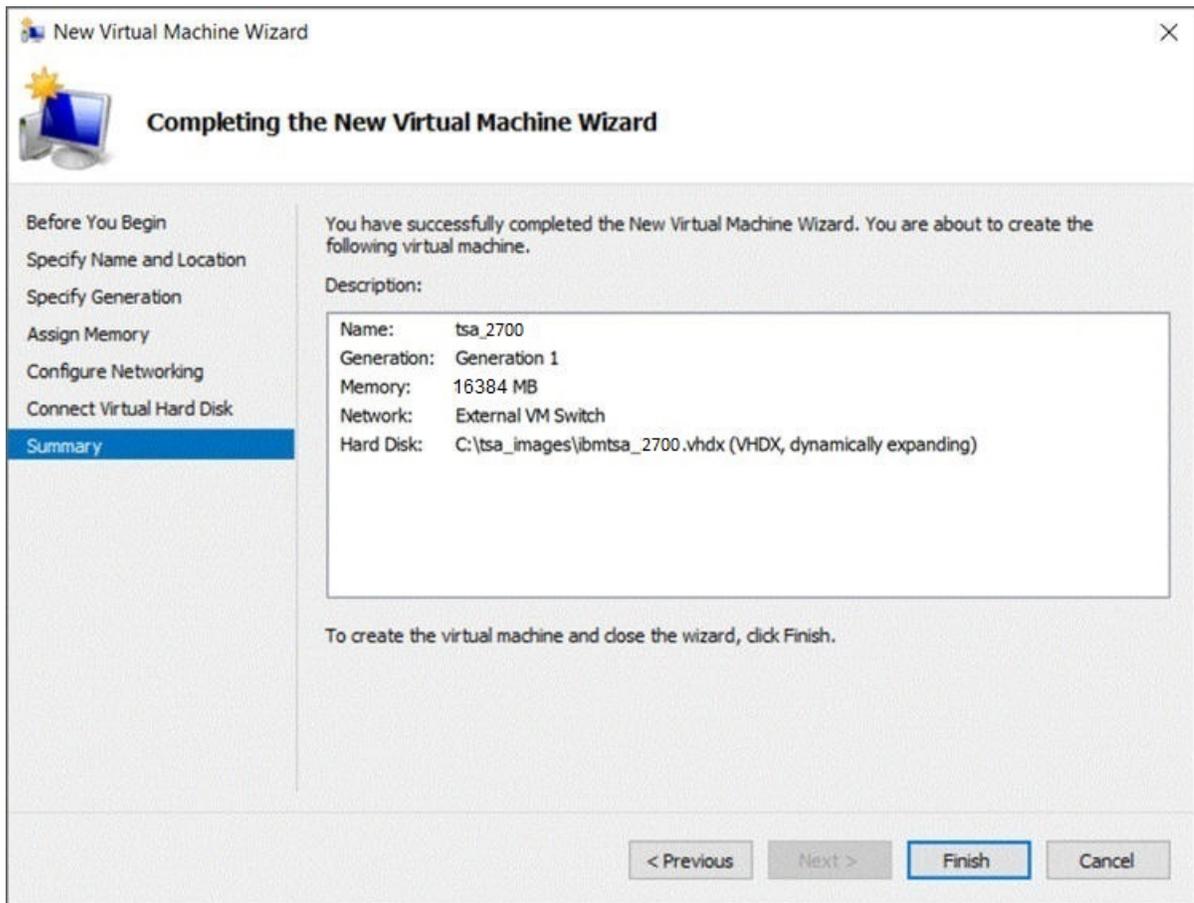


Figura 13. Riepilogo

- La nuova macchina virtuale viene aggiunta in Hyper-V Manager. Selezionare la macchina virtuale, passare al menu **Azioni** e fare clic su **Avvia**.

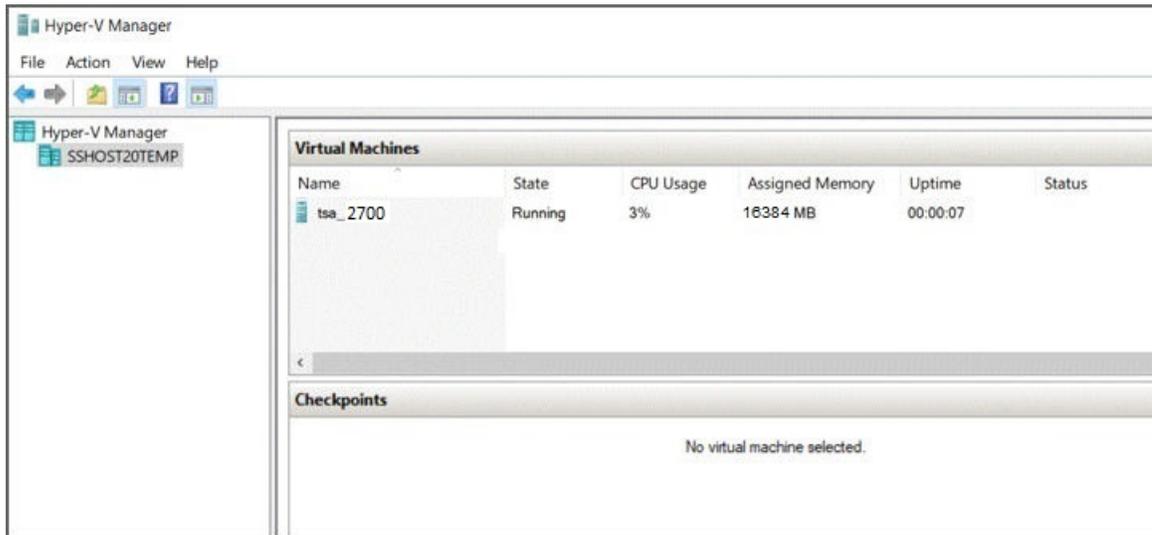


Figura 14. Hyper-V Manager

- Dal menu **Azioni**, selezionare **Connetti** per avviare una sessione della console. Nella console di TSA, immettere **ibmtsa login** come **tsausr** e **Password** come **configTsa**.
- Richiesto: Per modificare la password di accesso, continuare con i passi elencati nella sezione “Modifica della password per tsausr (obbligatorio)” a pagina 19.
- Per completare l'installazione, continuare con i passi elencati nella sezione “Configurazione dei dettagli di rete” a pagina 19.

Modifica della password per *tsaur* (obbligatorio)

Per scopi di sicurezza, è consigliato modificare la password per *tsaur* dal valore iniziale. Attenersi alla seguente procedura per modificare la password per *tsaur*.

Procedura

1. Selezionare l'opzione **2) Modifica password per *tsaur*** dal **menu di configurazione TSA**.

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsaur password
3) Set Appliance certificate to default
4) Exit

Choose an option: 2
```

Figura 15. Modifica password

2. Immettere la nuova password nel campo **Nuova password**. Immettere la stessa password nel campo **Digitare nuovamente la nuova password**. La nuova password deve avere una lunghezza di almeno 7 caratteri.

```
Changing password for user tsaur.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Returning to menu in 5 seconds...
```

Figura 16. Nuova password

Configurazione dei dettagli di rete

Procedura

1. Selezionare l'opzione **1) Impostazione della configurazione di rete** dal **menu di configurazione TSA**.

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsaur password
3) Set Appliance certificate to default
4) Exit

Choose an option: _
```

Figura 17. Impostazione della configurazione di rete

2. Immettere i seguenti dettagli della configurazione di rete.

```

Enter IPTYPE={static|dhcp}:static
Enter Hostname(default=ibmtsa):ibmappliance
Enter IP Address:10.10.10.10
Enter Netmask:255.255.255.255
Enter Gateway Address:10.10.10.1
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:static
HOSTNAME:ibmappliance
IPADDR:10.10.10.10
NETMASK:255.255.255.255
GATEWAY:10.10.10.1
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:_

```

Figura 18. Configurazione di rete

- a) **Immettere IPTYPE = {static|dhcp}**. Immettere static o dhcp. Nel caso di static, attenersi alla seguente procedura; in caso contrario, completare la procedura di configurazione di dhcp nella sezione [Appendice C, “Configurazione dei dettagli di rete DHCP”](#), a pagina 135

IPTYPE: static

Immettere il nome host (valore predefinito=ibmtsa). È possibile modificare il nome host predefinito. Assicurarsi che il nome host utilizzato sia univoco.

Immettere l'indirizzo IP.

Immettere la maschera di rete e Immettere il gateway.

Immettere il dominio di rete del sistema per l'utilizzo DNS (facoltativo).

Immettere DNS 1 (facoltativo), Immettere DNS 2 (facoltativo) e Immettere DNS 3 (facoltativo).

I dettagli della configurazione di rete specificati vengono visualizzati per la conferma.

- b) Immettere **[y|n]** per confermare o eliminare la configurazione di rete. Immettendo **y**, la configurazione di rete viene salvata e il sistema viene riavviato automaticamente.

Nota: Per le eventuali configurazioni non corrette, è possibile modificare i dettagli. Immettere **n** per ignorare le impostazioni correnti e riavviare la configurazione dal passo “2.a” a pagina 20

- c) Affinché la nuova configurazione di rete abbia effetto, il sistema viene riavviato dopo 15 secondi.

- d) Accedere a TSA dal browser utilizzando HTTP sicuro con il nome host o l'indirizzo IP immessi in precedenza.

Ad esempio, <https://<nomehost | indirizzo IP>>.

Nota: Durante la prima connessione, il browser potrebbe visualizzare un'eccezione di sicurezza. È necessario accettare il certificato di sicurezza e proseguire con l'accesso a TSA.

Nota: Per modificare le impostazioni di rete di base per TSA tramite l'interfaccia utente, seguire la procedura in [“Configurazione delle impostazioni di rete di base”](#) a pagina 36. Per configurare le impostazioni di rete avanzate, seguire la procedura in [“Configurazione delle impostazioni di rete avanzate”](#) a pagina 38.

3. Configurare Technical Support Appliance seguendo i passi elencati nella sezione [Capitolo 4, “Configurazione di Technical Support Appliance”](#), a pagina 23

Risultati

Una volta configurato correttamente TSA, consultare [Capitolo 5, “Configurazione del rilevamento e della trasmissione a IBM”](#), a pagina 51

Capitolo 4. Configurazione di Technical Support Appliance

Informazioni su questa attività

Attenersi alla seguente procedura per iniziare velocemente con TSA. Consultare l'argomento [Capitolo 2, "Prerequisiti"](#), a pagina 5, se non già fatto.

Procedura

1. ["Accesso a Technical Support Appliance"](#) a pagina 23
2. ["Accettazione dell'Accordo di licenza"](#) a pagina 25
3. ["Utilizzo della Procedura guidata di configurazione per la configurazione iniziale"](#) a pagina 27
 - a) ["Configurazione della connettività IBM"](#) a pagina 28
 - b) ["Registrazione di Technical Support Appliance"](#) a pagina 29
 - c) ["Impostazione dell'orologio"](#) a pagina 31
 - d) ["Configurazione della pianificazione della trasmissione"](#) a pagina 33
 - e) ["Aggiornamento di Technical Support Appliance"](#) a pagina 34
4. ["Configurazione delle impostazioni di rete"](#) a pagina 35
5. ["Configurazione dei certificati"](#) a pagina 44.
6. Opzionale: [Appendice D, "Account utente e gruppi di utenti"](#), a pagina 137

Operazioni successive

Una volta terminata la configurazione di TSA, consultare [Capitolo 5, "Configurazione del rilevamento e della trasmissione a IBM"](#), a pagina 51 per informazioni su come eseguire altre attività.

Accesso a Technical Support Appliance

Procedura

1. Aprire un browser internet da un sistema con accesso di rete a TSA.
Per ulteriori informazioni, consultare ["Browser web richiesti"](#) a pagina 5.
2. Immettere il seguente URL nella barra degli indirizzi del browser:

```
https://<nomehost o indirizzo IP>
```

Nota: Se il <nomehost> non funziona, provare con l'indirizzo IP assegnato di TSA.

3. Quando richiesto, immettere le seguenti informazioni:

ID utente:

Immettere admin

Password:

Immettere la password dell'amministratore di TSA.

La password iniziale è passw0rd. È necessario modificare la password iniziale dopo l'accesso a TSA.

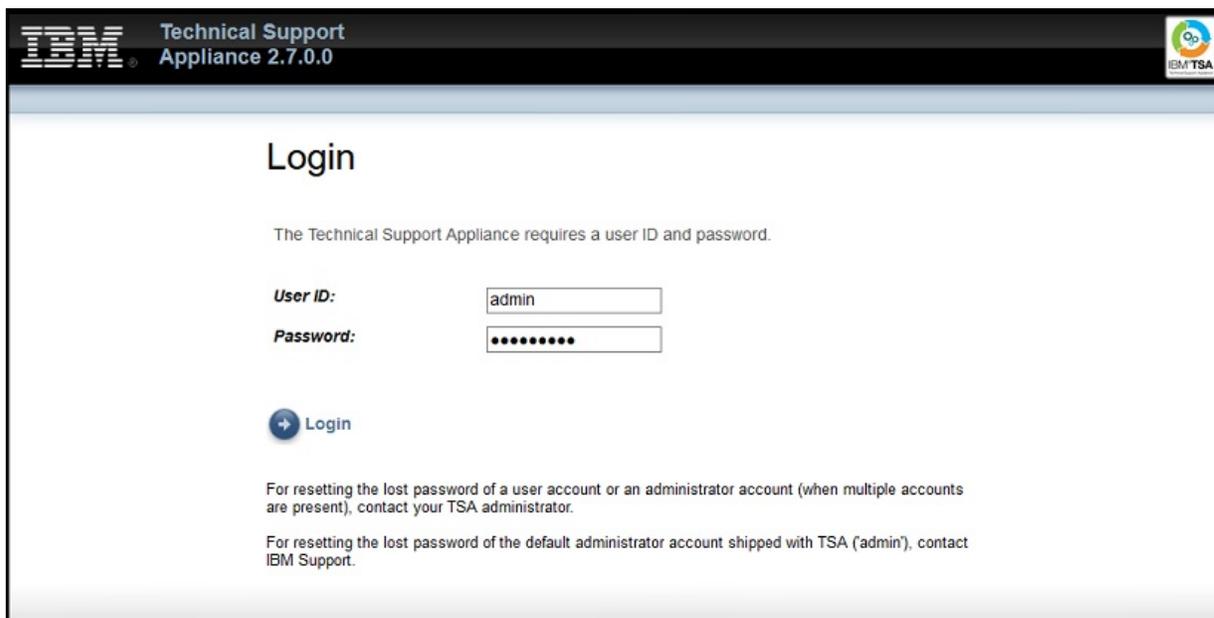


Figura 19. Accedi

Al primo accesso, viene visualizzata la pagina **Modifica password**.

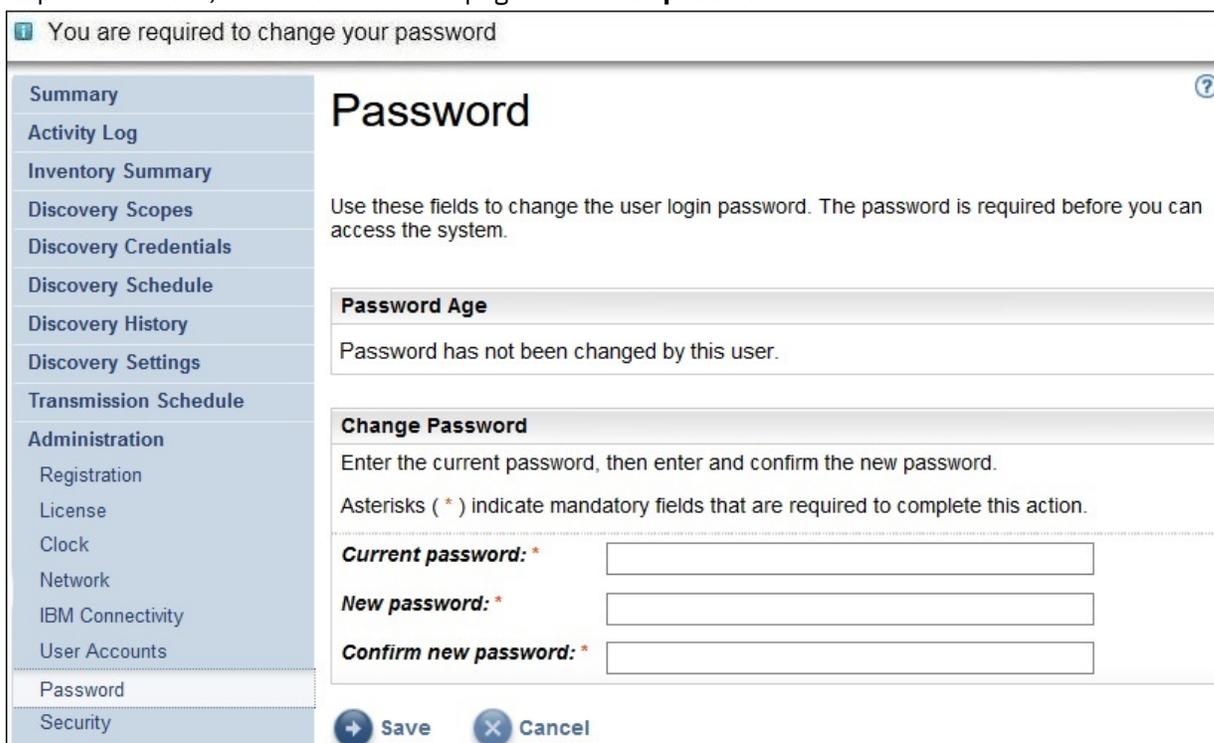


Figura 20. Modifica password

Per modificare la password iniziale, attenersi alla seguente procedura:

a) Immettere una nuova password.

La password deve rispettare le seguenti regole:

- Deve essere lunga almeno 8 caratteri
- Deve contenere almeno un carattere alfabetico e un carattere non alfabetico
- Non deve contenere il nome utente

- Non deve essere uguale a una delle precedenti otto password
 - Deve essere modificata almeno una volta ogni 90 giorni, ma non deve essere modificata più di una volta al giorno
- b) Immettere ancora la nuova password nel campo **Conferma nuova password**.
Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.
- c) Registrare la nuova password per riferimenti futuri.
- Importante:** Non è possibile ripristinare una password, pertanto se la si perde o dimentica, non è possibile accedere a TSA per modificare le credenziali. Se si perde o si dimentica la password per un account utente o account amministratore (se si dispone di più account), contattare l'amministratore TSA. Se si perde o si dimentica la password per l'account amministratore predefinito (inviato con TSA), contattare il supporto IBM.
- d) Fare clic su **Salva**. Al primo accesso, viene visualizzata la pagina **Accordo di licenza**.

Accettazione dell'Accordo di licenza

Per proseguire, leggere e accettare l'accordo di licenza.

Summary	<h1>License Agreement</h1> <p>Read the following license agreements carefully and Accept to proceed further.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>IBM Base License Agreement</p> <p style="text-align: center;">International License Agreement for Non-Warranted Programs</p> <p>Part 1 - General Terms</p> <p>BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,</p> <p>* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND</p> <p>* PROMPTLY RETURN THE UNUSED MEDIA AND DOCUMENTATION TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.</p> <p>1. Definitions</p> <p>"Authorized Use" - the specified level at which Licensee is authorized to execute or run the Program. That level may be measured by number of users, millions of service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use specified by IBM.</p> <p>"IBM" - International Business Machines Corporation or one of</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>IBM License and Statement of Work</p> <p style="text-align: center;"> View IBM License and Statement of Work </p> <p style="text-align: center; margin-top: 10px;"> Accept </p> </div>
Activity Log	
Inventory Summary	
Discovery Scopes	
Discovery Credentials	
Discovery Schedule	
Discovery History	
Discovery Settings	
Transmission Schedule	
Administration	
Tools	
Documentation	

Figura 21. Accordo di licenza

L'Accordo di licenza include i seguenti elementi:

- **Accordo di licenza di base IBM:** Visualizza l'accordo di licenza di base IBM.
- **Licenza IBM e descrizione dei lavori:** fare clic su **Visualizza Licenza IBM e descrizione dei lavori** per visualizzare la licenza IBM e la descrizione dei lavori.

Nota: TSA è conforme con il GDPR [EU/2016/679]. È possibile visualizzare le informazioni sulla conformità con il GDPR nella sezione **Licenza IBM e descrizione dei lavori**.

- **Informazioni e avvisi IBM:** fare clic su **Visualizza Informazioni e avvisi IBM** per visualizzare le informazioni e gli avvisi IBM.
- **Termini e condizioni per il codice di licenza separato:** fare clic su **Visualizza termini e condizioni per il codice di licenza separato** per visualizzare i termini e le condizioni per il codice di licenza separato.

Fare clic su **Accetta** per accettare l'accordo. Una volta accettata la licenza, viene visualizzata la **Procedura guidata di configurazione** per configurare TSA. È possibile configurare TSA tramite la **Procedura guidata di configurazione** o è possibile uscire dalla procedura guidata e configurare le impostazioni di TSA in base ai requisiti.

Nota: Nel pannello di navigazione, fare clic su **Amministrazione** > **Licenza** per visualizzare l'Accordo di licenza più recente accettato.

Concetti correlati

“Utilizzo della Procedura guidata di configurazione per la configurazione iniziale” a pagina 27
Utilizzare la **Procedura guidata di configurazione** per la configurazione iniziale di TSA.

“Configurazione di Technical Support Appliance” a pagina 125

Se si esce o si salta la configurazione di una delle impostazioni nella **procedura guidata di configurazione**, è possibile configurarle manualmente dal menu di navigazione a sinistra in TSA.

Utilizzo della Procedura guidata di configurazione per la configurazione iniziale

Utilizzare la **Procedura guidata di configurazione** per la configurazione iniziale di TSA.

Dopo aver accettato l'accordo di licenza, viene visualizzata automaticamente la **Procedura guidata di configurazione**.

Nota: Per avviare manualmente la **Procedura guidata di configurazione**, nel pannello di navigazione, fare clic su **Strumenti** > **Procedura guidata di configurazione** > **Avvia procedura guidata di configurazione**.



Figura 22. Procedura guidata di configurazione

La **Procedura guidata di configurazione** guida l'utente nelle seguenti operazioni:

- “Configurazione della connettività IBM” a pagina 28
- “Registrazione di Technical Support Appliance” a pagina 29
- “Impostazione dell'orologio” a pagina 31
- “Configurazione della pianificazione della trasmissione” a pagina 33

- “Aggiornamento di Technical Support Appliance” a pagina 34

Nota: Se si esce o si salta la configurazione di una delle impostazioni nella **procedura guidata di configurazione**, è possibile configurarle manualmente dal pannello di navigazione di TSA. Per maggiori informazioni sulla configurazione di queste impostazioni, consultare [Appendice B, “Configurazione di Technical Support Appliance”](#), a pagina 125.

Configurazione della connettività IBM

Procedura

È possibile visualizzare, modificare e verificare la configurazione che TSA utilizza per la connessione a IBM.

Figura 23. Connettività IBM

1. Nel pannello **Accesso**, effettuare la selezione tra i seguenti tipi di accesso Internet:

Consenti connessione SSL diretta

TSA si connette a IBM mediante connessione diretta.

Utilizza connessione proxy SSL

TSA si connette IBM mediante connessione proxy SSL.

Utilizza connessione proxy SSL di autenticazione

TSA si connette a IBM mediante una connessione proxy SSL di autenticazione.

2. Se è stato selezionato **Utilizza connessione proxy SSL** o **Utilizza connessione proxy SSL di autenticazione**, specificare le seguenti informazioni per il server proxy.

Indirizzo IP o nome host

L'indirizzo IP o il nome host del server proxy.

Nota: Il nome host immesso non deve contenere caratteri di sottolineatura ("_").

Porta

Il numero di porta del server proxy.

3. Se è stato selezionato **Utilizza connessione proxy SSL di autenticazione**, specificare le seguenti informazioni per il server proxy:

Nome utente

Il nome utente che il server proxy richiede per l'autenticazione.

Password

La password associata al nome utente che il server proxy richiede per l'autenticazione.

Conferma password

Reimmettere la password. Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.

Operazioni successive

- Fare clic su **Salva & Verifica connessione** per salvare e verificare la connessione specificata. Se la connessione riesce, viene visualizzato il pulsante **Continua**.
- Fare clic su **Continua** per andare alla pagina **Registrazione**.
- o-
- Fare clic su **Esci dalla procedura guidata** per uscire dalla **Procedura guidata di configurazione** e andare alla pagina **Riepilogo**.

Registrazione di Technical Support Appliance

È possibile visualizzare e modificare l'ubicazione fisica e il contatto di servizio del sistema.

Procedura

Registration

This page allows you to view and change the system service contact and physical location information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Service Contact

Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

Company name: *
Name of the organization that owns or is responsible for this system.

Contact name:
Name of the person in your organization who is responsible for repairs and maintenance of the system.

Telephone number:
Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.

Email:
Email address of the contact person.

IBMid:
You can log on to the [IBM Client Insights Portal](#) with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to <https://www.ibm.com/account> to sign up.

System Location

Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.

Country or region: *
The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

State or province: *
The state or province where the system is located.

Postal code: *
The postal code where the system is located.

City: *
The city or locality where the system is located.

Street address: *
The first line of the system location address.

Telephone number:
The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.

Building, floor, office:
The building, floor, and office where the system is located.

Figura 24. Registrazione

1. Specificare le informazioni sul contatto di servizio nei seguenti campi:

Nome società

Il nome dell'organizzazione che utilizza TSA.

Nome contatto

(Facoltativo) Il nome della persona dell'organizzazione che è responsabile per TSA.

Numero di telefono

(Facoltativo) Il numero di telefono al quale può essere raggiunta la persona di contatto. Il numero di telefono deve includere il prefisso locale, il numero di scambio e l'interno. Non utilizzare le parentesi nei numeri di telefono.

Email

(Facoltativo) L'indirizzo email della persona di contatto.

IBMid

(Facoltativo) L'IBMid della persona che si desidera autorizzare a visualizzare i report su IBM Client Insights Portal.

Nota: È possibile accedere a <https://clientinsightsportal.ibm.com/> con il proprio IBMid associato per scaricare i report TSA in 1-2 giorni dopo ogni trasmissione di dati. Per registrarsi per un IBMid, andare all'indirizzo <https://www.ibm.com/account>.

Nota: Il contatto di servizio identifica la persona che il supporto IBM deve contattare se c'è un problema con il sistema. Le informazioni di contatto sono utilizzate per assistere IBM nel fornire all'azienda i risultati dell'analisi Technical Support Appliance.

2. Specificare le informazioni sull'ubicazione del TSA nei seguenti campi:

Paese o regione

Il paese o la regione in cui si trova il TSA.

Stato o provincia

Lo stato o la provincia in cui si trova il TSA. Se non si è certi dello Stato, immettere *Sconosciuto*

Codice postale

Il codice postale relativo all'ubicazione del TSA.

Città

La città o località in cui si trova il TSA.

Indirizzo

L'indirizzo dell'ubicazione del TSA.

Numero di telefono

(Facoltativo) Il numero di telefono della stanza in cui si trova il TSA. Il numero di telefono deve includere il prefisso locale, il numero di scambio e l'interno. Non utilizzare le parentesi nei numeri di telefono.

Edificio, piano, ufficio

(Facoltativo) L'edificio, il piano e l'ufficio in cui si trova il TSA.

Operazioni successive

- Fare clic su **Salva & continua** per salvare le informazioni di registrazione e continuare con la pagina **Orologio**.
 - Fare clic su **Indietro** per tornare alla pagina **Connettività IBM**.
- 0-
- Fare clic su **Esci dalla procedura guidata** per uscire dalla **Procedura guidata di configurazione** e andare alla pagina **Riepilogo**.

Impostazione dell'orologio

È possibile impostare l'ora, la data e il fuso orario locale del sistema TSA durante la configurazione.

Procedura

IBM Connectivity
Registration
Clock
Transmission Schedule
Update

Clock

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Time Zone

Define the Greenwich Mean Time (GMT) offset corresponding to the time zone where this system is located and whether the system clock should automatically adjust when Daylight Savings Time (DST) changes.

GMT offset: * +0:00 - Greenwich Mean Time

DST adjustment: * Automatically adjust for daylight saving changes

Select Time Option

Select whether to use a local or public NTP (Network Time Protocol) server to update the system clock automatically or manually configure it.

Select: * Manually configured system clock

Date and Time

Manually set the system date and time.

Date (mm/dd/yyyy): * 03/02/2020
Defines the manually set system date.

Time (hh:mm:ss): * 16:26:16
Defines the manually set system time.

NTP Settings

Defines the IP addresses or hostnames of up to 2 Network Time Protocol servers for system clock synchronization.

NTP server 1: *
Defines the IP address or hostname for NTP server 1.

NTP server 2:
Defines the IP address or hostname for NTP server 2.

Back Save & Continue Skip Exit Wizard

Figura 25. Orologio

1. Selezionare il fuso orario locale dall'elenco a discesa **Differenza GMT**.
2. Selezionare l'adattamento dell'ora legale (o DST - daylight saving time) dall'elenco a discesa **Modifica DST**.

Nota: Non tutti i fusi orari consentono l'ora legale. Se si seleziona questa opzione per un fuso orario che non consente l'ora legale, viene visualizzato un errore.

3. Selezionare un metodo per aggiornare l'orologio di sistema dall'elenco a discesa **Seleziona opzione ora**.

Le opzioni includono la sincronizzazione dell'orologio di sistema con un server NTP (Network Time Protocol) per aggiornare automaticamente l'orologio di sistema o configurarlo manualmente.

- a) Se si sceglie di configurare manualmente l'orologio di sistema, è necessario impostare la data e l'ora del sistema. Immettere le informazioni di data e ora nei campi **Data** e **Ora**.
- b) Se si sceglie di sincronizzare l'orologio di sistema con un server NTP (Network Time Protocol) per aggiornare automaticamente l'orologio di sistema, è necessario specificare gli indirizzi IP e i nomi host dei server NTP. Immettere le informazioni per indirizzo IP o nome host per un massimo di due server nei campi **Server NTP**.

Nota: Assicurarsi che il server NTP sia accessibile tramite la rete per TSA.

Operazioni successive

- Fare clic su **Salva & continua** per salvare le informazioni dell'orologio e continuare con la pagina **Pianificazione trasmissione**.

-0-

- Fare clic su **Ignora** per passare alla pagina **Pianificazione trasmissione**.

Per modificare le impostazioni sul passo precedente della procedura guidata

- Fare clic su **Indietro** per tornare alla pagina **Registrazione**.

Per uscire dalla procedura guidata

- Fare clic su **Esci dalla procedura guidata** per uscire dalla **Procedura guidata di configurazione** e andare alla pagina **Riepilogo**.

Configurazione della pianificazione della trasmissione

TSA fornisce una pianificazione predefinita in base alla quale eseguire il processo di trasmissione a un determinato orario. È possibile modificare questa pianificazione in base alle esigenze.

Procedura

1. Utilizzare gli elenchi a discesa **A ore** e **A minuti** per selezionare il nuovo orario.
2. Selezionare **Modalità di selezione giorno**.

Per giorno settimanale (dom-sab)

Per pianificare la trasmissione in giorni specifici di una settimana, selezionare l'opzione **Per giorno settimanale (dom-sab)**.

Figura 26. Per giorno settimanale (dom-sab)

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni della settimana.

Per data mensile (1-31)

Per pianificare la trasmissione in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni del mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

Nota: Assicurarsi che l'ora di inizio del rilevamento sia anteriore all'ora di trasmissione, per evitare lunghi ritardi nella trasmissione dei dati appena raccolti.

Operazioni successive

- Fare clic su **Salva & continua** per salvare la pianificazione della trasmissione e continuare con la pagina **Aggiorna**.

-0-

- Fare clic su **Ignora** per passare alla pagina **Aggiorna**.

Per modificare le impostazioni sul passo precedente della procedura guidata

- Fare clic su **Indietro** per tornare alla pagina **Orologio**.

Per uscire dalla procedura guidata

- Fare clic su **Esci dalla procedura guidata** per uscire dalla **Procedura guidata di configurazione** e andare alla pagina **Riepilogo**.

Aggiornamento di Technical Support Appliance

È possibile aggiornare TSA all'ultima versione disponibile.

Se è disponibile un aggiornamento, viene visualizzata la seguente pagina **Aggiornamento**.

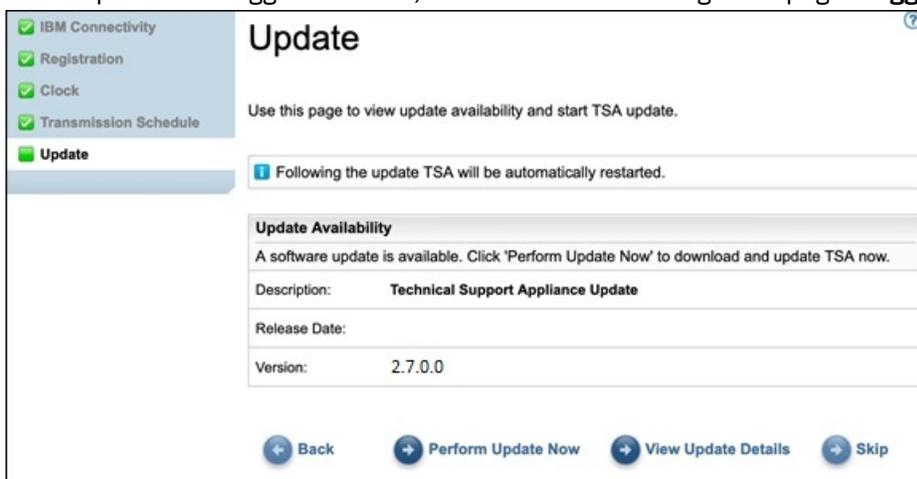


Figura 27. Disponibilità degli aggiornamenti

- Fare clic su **Esegui ora l'aggiornamento** per installare l'aggiornamento e completare la **Procedura guidata di configurazione**.

-0-

- Fare clic su **Visualizza dettagli dell'aggiornamento** per visualizzare le informazioni sul contenuto dell'aggiornamento.

Per modificare le impostazioni sul passo precedente della procedura guidata

- Fare clic su **Indietro** per tornare alla pagina **Pianificazione trasmissione**.

Per completare la procedura guidata

- Fare clic su **Ignora** per completare la **procedura guidata di configurazione** senza applicare l'aggiornamento.

Se non è disponibile un aggiornamento, viene visualizzata la seguente pagina **Aggiornamento**.

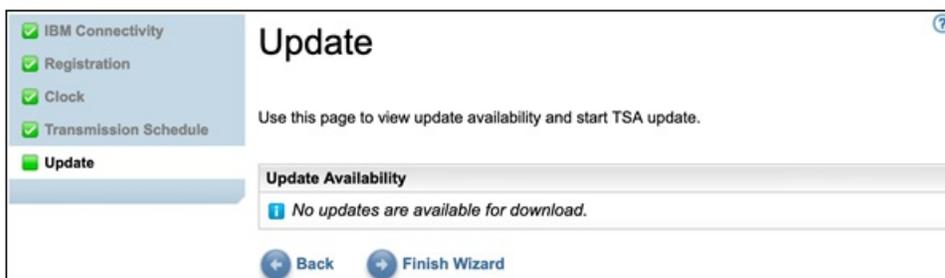


Figura 28. Nessun aggiornamento disponibile

- Fare clic su **Termina la procedura guidata** per completare la **Procedura guidata di configurazione**. Viene visualizzata la pagina **Procedura guidata di configurazione completata**.

-0-

- Fare clic su **Indietro** per tornare alla pagina **Pianificazione trasmissione**.

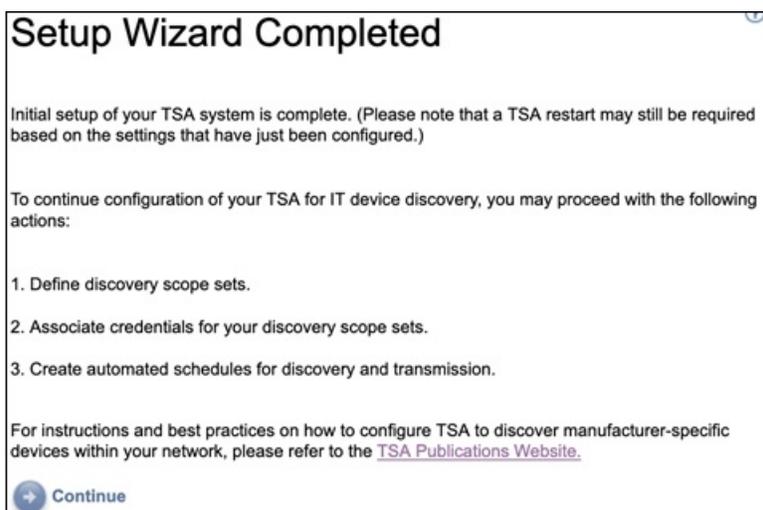


Figura 29. Procedura guidata di configurazione completata

- Fare clic su **Continua** per andare alla pagina **Riepilogo**.

Nota: Alcune modifiche nella pagina **Orologio** richiedono il riavvio per diventare effettive. Ad esempio, se è stata impostata la data o l'ora, o si passa dalla configurazione manuale alla configurazione del server NTP, viene richiesto di riavviare il server.

- Fare clic su **OK** per terminare la **Procedura guidata di configurazione** e tornare alla pagina **Riepilogo**. Viene visualizzata la pagina **Riepilogo** e il sistema si riavvia.

Nota: Se si esce o si salta la configurazione di una delle impostazioni nella **procedura guidata di configurazione**, è possibile configurarle manualmente dal pannello di navigazione di TSA. Per maggiori informazioni sulla configurazione di queste impostazioni, consultare [Appendice B, “Configurazione di Technical Support Appliance”](#), a pagina 125.

Configurazione delle impostazioni di rete

L'installazione di TSA richiede la configurazione delle impostazioni di rete di base. Se queste impostazioni sono adatte per la propria rete IT, è possibile ignorare questa sezione.

Prima di iniziare

Utilizzare la pagina **Rete** per effettuare una delle seguenti azioni:

- Modificare le impostazioni di rete di base iniziali

- Configurare TSA per accedere a più reti

Per configurare le impostazioni di rete di base tramite la console, seguire i passi nella sezione [“Configurazione dei dettagli di rete”](#) a pagina 19.

Configurazione delle impostazioni di rete di base

Utilizzare la pagina **Rete** per modificare le impostazioni di rete iniziali.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Rete**.
Viene visualizzata la pagina **Rete**.

- Summary
- Activity Log
- Inventory Summary
- Discovery Scopes
- Discovery Credentials
- Discovery Schedule
- Discovery History
- Discovery Settings
- Transmission Schedule
- Administration
 - Registration
 - Clock
- Network
- IBM Connectivity
- User Accounts
- Password
- Security
- Backup and Restore
- Update
- Logging and Trace
- Scheduled Maintenance
- Shutdown
- Tools
- Documentation

Related links

- Advanced network

Network ?

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *
The network unique identifying name for this system.

Domain name suffix: *
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Gateway address: *
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: *

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: *
Defines the IP address for the DNS server to search 1st.

DNS server 2:
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Figura 30. Rete

2. Nel campo **Nome host**, specificare il nome univoco per questo sistema sulla rete locale.
3. Nel campo **Suffisso nome dominio**, specificare il nome utilizzato come nome dominio per questo sistema sulla rete locale.

4. Selezionare **Usa IP statico configurato manualmente** per *Assegnazione IP*. Per l'assegnazione dell'indirizzo DHCP, consultare la sezione Appendice C, "Configurazione dei dettagli di rete DHCP", a pagina 135.
 5. Configurare l'indirizzo IP statico:
 - a) Nel campo **Indirizzo IP**, immettere l'indirizzo IP per questo sistema.
 - b) Nell'elenco a discesa **Subnet mask**, selezionare la subnet mask che questo sistema deve utilizzare.
 - c) Nel campo **Indirizzo gateway**, immettere l'indirizzo IP del sistema o router che gestisce le richieste al di fuori della subnet corrente.
 6. Specificare i **Servizi nome** in base all'assegnazione IP.
 - a) Per gli IP statici configurati manualmente, selezionare l'opzione **Utilizza DNS, utilizzando indirizzi server di seguito**.
 - b) Per l'assegnazione indirizzo IP DHCP, selezionare l'opzione **Utilizza DNS, ma ottieni indirizzi server tramite DHCP**.
 7. Immettere fino a tre indirizzi IP che i server DNS (Domain Name System) possono utilizzare quando si risolvono i nomi host.

TSA cerca i server nell'ordine in cui sono visualizzati.
 8. Fare clic su **Salva** per salvare le impostazioni di rete.

Viene richiesto di riavviare il sistema.
-  **Avvertenza:** Prestare attenzione quando si modificano le impostazioni di rete. Se si fa un errore con la configurazione di rete la IU TSA potrebbe non essere raggiungibile. In tal caso, deve essere utilizzata la console TSA per correggere la configurazione di rete:
- Per VMware, utilizzare l'interfaccia web VMware ESXi o il client VMware vSphere
 - Per Microsoft Hyper-V, utilizzare Hyper-V Manager
9. Fare clic su **Annulla** per uscire dalla pagina **Rete** senza salvare le impostazioni.

Configurazione delle impostazioni di rete avanzate

Se si desidera configurare TSA per accedere a più reti, utilizzare la pagina **Rete (avanzate)** per specificare tali impostazioni di rete.

Per configurare le impostazioni di rete avanzate, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione > Rete**.
2. Nel pannello di navigazione inferiore, sotto **Collegamenti correlati**, fare clic su **Rete avanzata**.

Network

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *
The network unique identifying name for this system.

Domain name suffix: *
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Gateway address: *
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: *

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: *
Defines the IP address for the DNS server to search 1st.

DNS server 2:
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

[- Advanced network](#)

Figura 31. Accedere alla pagina Rete (avanzate)

Viene visualizzata la pagina **Rete (avanzate)**.

La pagina **Rete (avanzate)** è suddivisa nelle seguenti pagine separate:

- Globale
- Interfacce di rete
- Impostazioni DNS
- Route di rete

Per accedere a queste singole pagine, fare clic sulla scheda per la pagina che si desidera visualizzare.

Importante: Fare clic su **Salva** prima di lasciare la pagina, per salvare le modifiche effettuate ai campi nella pagina. Viene richiesto di riavviare il sistema per rendere effettive le modifiche.

Globale

Utilizzare questa pagina per visualizzare e modificare le impostazioni di rete globali:

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global | Network Interfaces | DNS Settings | Network Routes

Use this page to view and change global system network settings.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *	<input type="text" value="host10e"/> <small>The network unique identifying name for this system.</small>
Domain name suffix: *	<input type="text" value="abc.def.com"/> <small>The name assigned as the domain name for this system.</small>

[Save](#)

Figura 32. Rete (avanzate) - Globale

Identità

Definire l'identità di questo sistema sulla rete.

1. Nel campo **Nome host**, specificare il nome univoco per questo sistema.
2. Nel campo **Suffisso nome dominio**, specificare il nome utilizzato come nome dominio per questo sistema.

Interfacce di rete

TSA è configurato per avere due NIC (Network Interface Controller) - eth0 e eth1. Utilizzare questa pagina per visualizzare e modificare le impostazioni correnti per l'interfaccia di rete selezionata.

1. Fare clic su **eth0** per selezionare l'interfaccia di rete eth0.
2. Fare clic su **eth1** per selezionare l'interfaccia di rete eth1.

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global **Network Interfaces** DNS Settings Network Routes

eth0 eth1

Use this page to view and change the current settings for the selected network interface.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Default Gateway Route

Select whether this interface provides the route to the default gateway.

Select: *

Default Gateway

Defines the IP address of the system/router that network requests will get routed to when no specific route exists.

Gateway address: *
IP address of the default gateway system.

[Save](#)

Figura 33. Rete (avanzate) - Interfacce di rete

Assegnazione IP

Selezionare un metodo per assegnare l'indirizzo IP per questo sistema. È possibile scegliere tra ottenere dinamicamente l'indirizzo IP da un server DHCP o utilizzare un indirizzo IP statico configurato manualmente. Se si sceglie di utilizzare un indirizzo IP statico configurato manualmente, è necessario configurare l'indirizzo IP di sistema su questa pagina.

Configurazione IP statico

Se si sceglie di configurare manualmente un indirizzo IP statico, specificare le informazioni IP per questa interfaccia di rete come segue:

1. Nel campo **Indirizzo IP**, specificare l'indirizzo IP per questo sistema.
2. Nell'elenco a discesa **Subnet mask**, selezionare la subnet mask che questo sistema deve utilizzare.

Route gateway predefinito

Specificare se questa interfaccia di rete fornisce una route al gateway predefinito.

Gateway predefinito

Nel campo **Indirizzo gateway**, specificare l'indirizzo IP del gateway predefinito per questo sistema.

Impostazioni DNS

Utilizzare questa pagina per visualizzare e modificare le impostazioni DNS.

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global Network Interfaces **DNS Settings** Network Routes

Use this page to view or change the Domain Name Services (DNS) settings.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: *

DHCP Interface

Select the network interface that is associated with DHCP server you wish to use.

Select interface: *

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: *
Defines the IP address for the DNS server to search 1st.

DNS server 2:
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Domain Suffix Search Order

Defines up to 3 domain suffixes to search for hostname resolution.

Domain suffix 1:
Defines the domain suffix to search 1st.

Domain suffix 2:
Defines the domain suffix to search 2nd.

Domain suffix 3:
Defines the domain suffix to search 3rd.

Figura 34. Rete (avanzate) - Impostazioni DNS

Servizi nome

Specificare un DNS (Domain Name System) sulla rete per convertire i nomi host in indirizzi IP. È possibile scegliere tra le seguenti opzioni:

- Utilizzare DNS, ma ottenere indirizzi server da un server DHCP.

Se si sceglie questa opzione, è necessario selezionare l'interfaccia di rete associata al server DHCP che si desidera utilizzare.

- Utilizzare DNS con indirizzi server che si specificano.

Se si sceglie questa opzione, è necessario specificare almeno un server DNS su questa pagina.

Interfaccia DHCP

Selezionare l'interfaccia di rete associata al server DHCP che si desidera utilizzare.

Ordine di ricerca server DNS

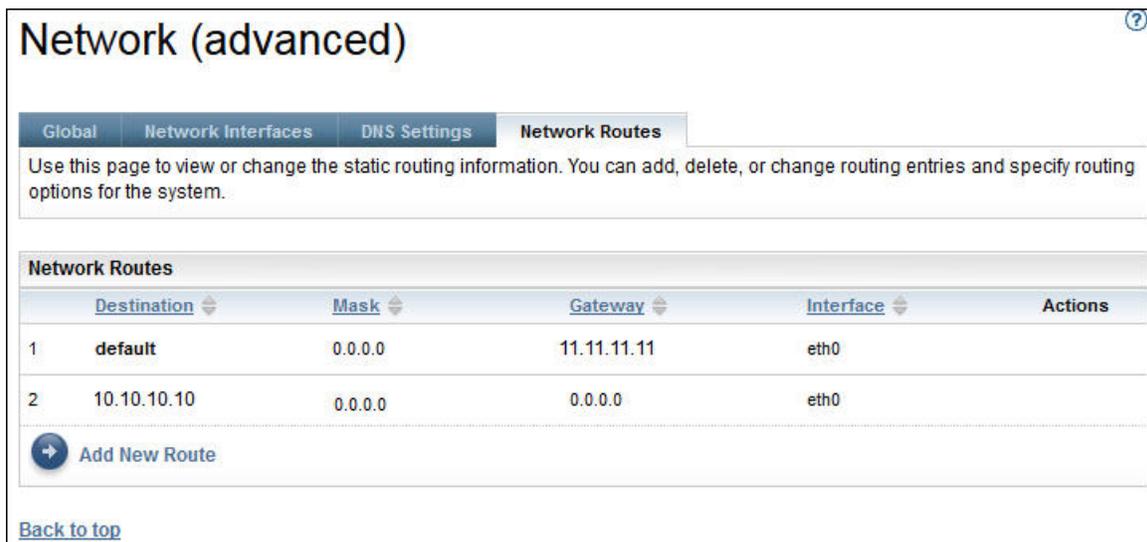
Se si sceglie di utilizzare DNS con indirizzi server che si specificano, immettere fino a tre indirizzi IP che i server DNS (Domain Name System) possono utilizzare quando risolvono i nomi host. TSA cerca i server nell'ordine in cui sono visualizzati.

Ordine di ricerca suffisso dominio

Se si sceglie di utilizzare DNS con indirizzi server che si specificano, immettere fino a tre suffissi nome dominio da utilizzare quando si risolvono i nomi host. TSA cerca questi suffissi nome dominio nell'ordine in cui sono visualizzati.

Route di rete

Utilizzare questa pagina per visualizzare, aggiungere, modificare o eliminare voci di instradamento statico.



Network Routes					
	Destination	Mask	Gateway	Interface	Actions
1	default	0.0.0.0	11.11.11.11	eth0	
2	10.10.10.10	0.0.0.0	0.0.0.0	eth0	

Figura 35. Rete (avanzate) - Route di rete

Sono visualizzate le seguenti informazioni per ogni route di rete:

Destinazione

Specifica l'indirizzo subnet o host di rete di destinazione TCP/IP.

Mask

Specifica la subnet mask da utilizzare come maschera di rete quando si aggiunge una route. Questo è l'indirizzo subnet per la porzione host dell'indirizzo IP. Le interfacce di rete possono utilizzare subnet mask differenti, fornendo la possibilità di aggiungere route selezionando una subnet mask (route subnet variabili). È necessario selezionare una subnet mask quando si aggiunge una route, in formato decimale con punti a 32 bit.

Gateway

Specifica l'indirizzo gateway TCP/IP per l'instradamento dei pacchetti IP.

Interfaccia

Selezionare l'adattatore dal menu. Questo è il nome dell'adattatore di rete associato alla voce tabella.

Azioni

Fare clic sull'icona **Elimina** per eliminare la route.

Nota: Le due route presentate nella [figura](#) non possono essere modificate o eliminate.

Fare clic su **Aggiungi nuova route** per definire una nuova route di rete statica. Viene visualizzata la pagina **Route di rete**.

Aggiunta delle route di rete

È possibile aggiungere route di rete statiche.

Procedura

Per aggiungere una route di rete, attenersi a questa procedura:

1. Sulla pagina **Rete (avanzate) - Route di rete**, fare clic su **Aggiungi nuova route**. Viene visualizzata la pagina **Route di rete**.

Network Route

Use this page to view or change the static routing information. You can add, delete, or change routing entries and specify routing options for the system.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Details

The following describes the static routing entry.

Destination: *
IP destination network host or subnet address.

Gateway: *
IP gateway address for routing the IP packets.

Subnet mask: *
The subnet mask for the host portion of the IP address.

Interface: *
Associated network interface for this route.

Figura 36. Nuova route di rete

2. Nel campo **Destinazione**, immettere l'indirizzo IP per la subnet o l'host di rete di destinazione TCP/IP.
3. Nel campo **Gateway**, immettere l'indirizzo gateway TCP/IP per l'instradamento delle informazioni. L'indirizzo deve essere in formato decimale con punti a 32 bit. Ad esempio: xxx . xxx . xxx . xxx.
4. Nell'elenco a discesa **Subnet mask**, selezionare la subnet mask da utilizzare come maschera di rete per questa route.
5. Dall'elenco a discesa **Interfaccia**, selezionare l'adattatore di rete da associare a questa route.
6. Fare clic su **Salva** per salvare questa route di rete.

Configurazione dei certificati

La pagina **Certificati** consente di visualizzare le informazioni di firma del certificato, generare e installare certificati o importare certificati. Questi sono i certificati server che TSA presenta a un server web quando si accede all'interfaccia utente.

La configurazione predefinita di TSA implementa un certificato server SSL autofirmato generico per facilitare la configurazione. Per maggiore sicurezza, si consiglia di sostituire il certificato predefinito dopo la distribuzione iniziale e il completamento delle operazioni di configurazione. È possibile utilizzare TSA per generare e installare un certificato server SSL autofirmato che sia univoco per questo TSA, generare e installare un certificato personalizzato che sia firmato da una autorità di certificazione di propria scelta o caricare il proprio file keystore Java contenente un certificato server SSL personalizzato.

È possibile installare un certificato personalizzato applicando uno dei seguenti metodi:

- “Installazione di un certificato personalizzato (utilizzando i firmatari)” a pagina 46
- “Installazione di un certificato personalizzato (metodo alternativo)” a pagina 47

Visualizzazione dello stato del certificato del server SSL

La configurazione di TSA installa il certificato TSA predefinito fornito con Technical Support Appliance.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Certificati**.

Viene visualizzata la pagina **Certificati**.

SSL Server Certificate Status	
Default SSL Server certificate is installed.	
Issued by:	CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US
Issued to:	CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US
Serial number:	4be3287b
Signature algorithm:	SHA256withRSA
Issued on:	Wednesday Apr 19 11:05:05 BST 2017
Expires on:	Thursday Apr 07 11:05:05 BST 2067

[Generate and install a new Self-Signed Certificate](#)

Figura 37. Stato certificato server SSL

La sezione **Stato certificato server SSL** visualizza informazioni sul certificato server SSL installato in TSA. Le informazioni sul certificato includono *Emesso da*, *Emesso per*, *Emesso il*, *Scade il*, *Numero di serie* e *Algoritmo di firma*.

2. Fare clic su **Genera e installa un nuovo certificato autofirmato** per installare un certificato autofirmato univoco per questo TSA. Viene visualizzato un messaggio di avvertenza che indica che l'appliance si riavvia automaticamente dopo la generazione e l'installazione di un certificato autofirmato.

Nota: Il pulsante **Genera e installa un nuovo certificato autofirmato** è visibile solo se su TSA è installato il certificato predefinito.

Generazione e scaricamento di una CSR

Per richiedere un certificato SSL che sia certificato da una CA (Certificate Authority), è necessario fornire le seguenti informazioni per generare e scaricare il file CSR (Certificate Signing Request).

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Certificati**.

Viene visualizzata la pagina **Certificati**.

Certificate Authority Signing Request

Enter the following information for the Certificate Signing Request(CSR) to be created:

Common Name: *

Organization Unit: *

Organization: *

City: *

State: *

Country: * The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

Number of days until expiration: *

[Generate and download Certificate Signing Request\(CSR\) file](#)

Figura 38. CSR (Certificate Signing Request)

2. Immettere il nome host completo (FQDN) di TSA nel campo **Nome comune**. Il limite minimo di caratteri è 1 e quello massimo è 64.
3. Specificare il nome organizzazione, che cambia tra i reparti in un'organizzazione nel campo **Unità organizzativa**.
4. Specificare il nome dell'azienda, società, università o agenzia governativa nel campo **Organizzazione**.
5. Specificare il nome della città o della località in cui è utilizzato TSA nel campo **Città**.
6. Specificare il nome dello stato o provincia in cui è utilizzato TSA nel campo **Stato**. Se non si è certi dello Stato, o se lo Stato non è applicabile per il proprio Paese, immettere *Sconosciuto*.
7. Selezionare il nome del Paese in cui è utilizzato TSA nell'elenco a discesa **Paese**.
8. Specificare il numero di giorni di validità del certificato, a partire dalla data di creazione del certificato nel campo **Numero di giorni alla scadenza**.
9. Fare clic su **Genera e scarica il file CSR (Certificate Signing Request)** per creare e scaricare il file CSR con le informazioni specificate.

Nota: Per ripristinare il certificato predefinito impacchettato con TSA, vedere la sezione [“Ripristino del certificato predefinito”](#) a pagina 48.

Installazione di un certificato personalizzato (utilizzando i firmatari)

Utilizzare questa funzione per installare un certificato personalizzato. È necessario il certificato server generato da una CA (Certificate Authority), il certificato radice per la CA e qualsiasi certificato intermedio per la CA.

Prima di iniziare

Assicurarsi che i file di certificato (certificato radice, intermedio e server) siano in uno dei seguenti formati

-
- *.crt*
- *.der*
- *.pem*

Procedura

Seguire questa procedura per caricare e installare i certificati su TSA:

1. Nel pannello di navigazione, fare clic su **Amministrazione > Certificati**.
Viene visualizzata la pagina **Certificati**.

Upload and install custom certificate using signers (a certificate chain)

Use this action to import multiple signers (a certificate chain) certificates and install a custom SSL server certificate from file.

To install a custom SSL certificate, import required multi-signers from file, then click "Upload ..."

Root certificate file: * No file chosen

Intermediate certificate file: No file chosen

Intermediate certificate file: No file chosen

Intermediate certificate file: No file chosen

TSA certificate file: * No file chosen

 **Upload and install a Custom Certificate using Certificates chain**

Figura 39. Installare il certificato personalizzato

2. Nel campo **File del certificato radice**, specificare l'ubicazione del file del certificato radice che si desidera installare su TSA.
3. Nel campo **File del certificato intermedio**, specificare l'ubicazione del file del certificato intermedio che si desidera installare su TSA.

Nota: Possono esistere più file di certificato intermedio (massimo 3) a seconda dei firmatari importati.

4. Nel campo **File del certificato TSA**, specificare l'ubicazione del file di certificato del server TSA che si desidera installare su TSA.
5. Fare clic su **Carica e installa un certificato personalizzato utilizzando la catena di certificati** per caricare tutti i file (*File del certificato radice*, *File del certificato intermedio*, *File del certificato TSA*) specificati e installare un certificato personalizzato utilizzando la catena di certificati.

Nota: Per ripristinare il certificato predefinito impacchettato con TSA, vedere la sezione [“Ripristino del certificato predefinito”](#) a pagina 48.

Installazione di un certificato personalizzato (metodo alternativo)

Utilizzare questa funzione per installare un certificato personalizzato. È possibile utilizzare questa funzione per distribuire un file keystore Java completo già creato.

Prima di iniziare

Si consiglia di utilizzare le funzioni **Richiesta di firma CA** e **Caricare e installare un certificato personalizzato utilizzando i firmatari (una catena di certificati)** dalla pagina **Certificati** per distribuire un certificato personalizzato. Tuttavia, se è già stato creato un file keystore Java completo indipendentemente (contenente le chiavi, il certificato personalizzato e i certificati CA pertinenti) è possibile utilizzare questa funzione per distribuire il file keystore. È necessario fornire l'ubicazione del file keystore e la password per il file.

Nota: Quando si crea il file keystore, assicurarsi che le password per la voce chiave e il keystore siano identiche.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Certificati**.
Viene visualizzata la pagina **Certificati**.

Figura 40. Installazione del certificato personalizzato

2. Per installare un certificato server personalizzato, attenersi alla seguente procedura.
 - a) Immettere la password per il certificato nel campo **Password certificato**.
 - b) Immettere nuovamente la password nel campo **Conferma password**.
Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.
 - c) Specificare l'ubicazione del file keystore Java che contiene il certificato personalizzato nel campo **File del certificato personalizzato**.
 - d) Fare clic su **Carica e installa il file JKS completo** per caricare il file keystore Java specificato e installare un certificato personalizzato. Il file keystore Java deve includere il certificato personalizzato e qualsiasi relativo certificato CA radice o intermedio. L'appliance si riavvia per attivare l'uso del nuovo certificato.

Nota: Per ripristinare il certificato predefinito impacchettato con TSA, vedere la sezione [“Ripristino del certificato predefinito”](#) a pagina 48.

Risultati

Una volta installato il nuovo certificato, TSA si riavvia automaticamente. Una volta completato il riavvio, il browser visualizza una richiesta di sicurezza relativamente all'attendibilità del nuovo certificato.

Ripristino del certificato predefinito

Per ripristinare il certificato predefinito impacchettato con TSA, utilizzare la console TSA e selezionare l'opzione **Imposta certificato predefinito appliance**.

Procedura

1. Avviare la console TSA.
2. Selezionare l'opzione **3) Imposta certificato predefinito appliance** dal **menu di configurazione TSA**.

Figura 41. Imposta certificato predefinito appliance

3. **Conferma impostazione del certificato predefinito dell'appliance [y|n]:** immettere **y** per confermare l'impostazione del certificato TSA sul certificato predefinito.

Risultati

Una volta installato il certificato predefinito, TSA si riavvia automaticamente entro 5 secondi. Una volta completato il riavvio, il browser visualizza una richiesta di sicurezza relativamente all'attendibilità del certificato predefinito.

Pianificazione della ripulitura dei dati di inventario

È possibile pianificare o eseguire manualmente un'attività di pulizia per tutti i dati di inventario raccolti sulle risorse, dal momento in cui sono stati rilevati.

Informazioni su questa attività



Attenzione: Si consiglia di eseguire l'attività di pulizia una volta a settimana per la maggior parte delle installazioni.

Per visualizzare la pianificazione corrente per l'attività di pulizia dell'inventario, selezionare **Riepilogo inventario** > **Pianificazione pulizia inventario**.

Inventory Cleanup Schedule

Inventory cleanup will purge dormant inventory data from the inventory database. Inventory elements that have not been discovered within the defined dormant age will be purged. This operation can be performed on demand or scheduled to run at specific times. A copy of the purged data is temporarily saved into the Inventory Cleanup Archive. To view the elements that have been purged within the last year, click on the Show Cleanup Archive button.

Inventory Summary	
Next run:	8/9/20 12:00 AM BST
Runs at:	12:00 AM on Sunday
Dormant age	60 days

History			
Status	Instance	State	Comments
✓	Inventory cleanup	Complete	<ul style="list-style-type: none">Last status: OKLast run: 8/2/20 12:00 AM BSTLast completed: 8/2/20 12:49 AM BSTLast duration: 49 minutes, 57 secondsInitiator: System

[Edit Schedule](#) [Run Inventory Cleanup Now](#) [Show Cleanup Archive](#)

Figura 42. Pianificazione pulizia inventario

Fare clic su **Esegui ora la pulizia dell'inventario** per eseguire manualmente la ripulitura dell'inventario. Per modificare, abilitare o disabilitare la pianificazione della pulizia inventario corrente, seguire questi passi:

Procedura

1. Sulla pagina **Pianificazione pulizia inventario**, fare clic su **Modifica pianificazione**.
2. Sulla pagina **Impostazioni inventario**, selezionare **Abilita pulizia inventario pianificata** per abilitare l'attività di pulizia inventario o su **Disabilita pulizia inventario pianificata** per disabilitarla.
3. Se si sceglie di abilitare l'attività di pulizia inventario, completare i seguenti passi:
 - a) Selezionare gli elenchi a discesa **A ore** e **A minuti** per selezionare il nuovo orario.
 - b) Selezionare **Modalità di selezione giorno**. Per pianificare la ripulitura dell'inventario in giorni specifici di una settimana, selezionare l'opzione **Settimanalmente per giorni (Dom - Sab)** o per

pianificare la ripulitura dell'inventario in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.

- c) Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere altri o differenti giorni della settimana o mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

4. Selezionare il periodo durante il quale si desidera conservare i dati di inventario dall'elenco **Periodo dormiente**.
5. Fare clic su **Salva**.

Capitolo 5. Configurazione del rilevamento e della trasmissione a IBM

Dopo il completamento della configurazione di TSA, è possibile utilizzare varie funzioni di amministrazione per gestire il rilevamento, la trasmissione e i lavori.

Ambiti di rilevamento

Un ambito di rilevamento specifica l'indirizzo IP, l'intervallo di indirizzi IP o la rete da utilizzare per rilevare elementi IT. Gli ambiti di rilevamento sono raggruppati in serie di ambiti di rilevamento.

TSA mette a disposizione vari tipi di ambiti di rilevamento:

- Serie di ambiti dinamici HMC - possono essere utilizzate per rilevare HMC insieme a tutte le partizioni da esse gestite.
- Serie di ambiti dinamici VMware - possono essere utilizzate per rilevare host VMware vCenter o ESXi, insieme a tutte le macchine virtuali sugli host ESXi.
- Ambiti di rilevamento generali - utilizzati per rilevare tutte le altre risorse non rilevate utilizzando una serie di ambiti dinamici. Gli indirizzi IP, l'intervallo di indirizzi IP o le reti si possono immettere manualmente oppure è possibile importare un elenco di indirizzi IP da un file in TSA.

Ambiti dinamici HMC

È possibile definire ambiti dinamici HMC per raccogliere inventari dettagliati dalle HMC, gli IBM Power System che gestiscono e anche le LPAR VIOS, AIX e Linux su quei sistemi.

Informazioni su questa attività

Oltre a richiamare le informazioni di inventario dalle HMC definite, TSA interroga anche le LPAR gestite da queste HMC dinamicamente, senza che si debba creare o gestire più definizioni di ambito. È necessario definire un ambito per le HMC e selezionare i tipi di LPAR (AIX, VIOS e Linux) che si desidera siano automaticamente scansionate quando vengono rilevate queste HMC. Il vantaggio è che, anche se le LPAR cambiano, non è necessario riconfigurare TSA.

The screenshot displays the 'HMC Dynamic Scopes' configuration page. On the left is a navigation sidebar with items such as Summary, Activity Log, Inventory Summary, Discovery Scales, and HMC Dynamic Scopes. The main content area features the title 'HMC Dynamic Scopes' and a descriptive paragraph: 'Users can define HMC Dynamic Scopes to collect detailed inventory from IBM Power Systems VIOS, AIX, and Linux LPARs. In addition to retrieving inventory information from the defined HMC, TSA also queries managed LPARs dynamically, without requiring users to create and maintain multiple scope definitions.' Below this is a table with the following structure:

Name	Actions
hmc_dynamic_1	[Edit] [Delete] [Add] [Refresh]

At the bottom of the table area, there is a '+ Add New HMC Dynamic Scope' button and a 'Back to top' link.

Figura 43. Ambiti dinamici HMC

Visualizzazione di ambiti dinamici HMC

È possibile visualizzare gli ambiti dinamici HMC esistenti.

Informazioni su questa attività

Per visualizzare gli ambiti dinamici HMC esistenti, fare clic su **Ambiti di rilevamento > Ambiti dinamici HMC** nel pannello di navigazione. Verrà visualizzata la pagina **Ambiti dinamici HMC**. Il pannello **Ambiti dinamici HMC** contiene un elenco di ambiti dinamici HMC.

Per visualizzare gli ambiti e le credenziali associate a una specifica serie di ambiti dinamici, fare clic sul nome della serie di ambiti nella colonna **Nome**. Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**.

HMC Dynamic Scope Set

General

Name: hmc_dynamic_1

HMC

Type	Value	Actions
Address	9.1.2.3	[Edit] [Delete] [Info]
Address	10.11.12.13	[Edit] [Delete] [Info]

+ Add HMC

HMC Credentials

Name	Type	User Name	Actions
hmc_1	Default	root	[Edit]

+ Add HMC Credentials

AIX Credentials

Name	Type	User Name	Actions
aix_1	Default	root	[Edit] [Delete] [Info]
aix_2	Default	root	[Edit] [Delete] [Info]

+ Add AIX Credentials

Linux Credentials

Name	Type	User Name	Actions
linux_1	Default	root	[Edit] [Delete]

+ Add Linux Credentials

VIOS Credentials

Name	Type	User Name	Actions
vios_1	Default	padmin	[Edit] [Delete]

+ Add VIOS Credentials

Figura 44. Visualizzare una serie di ambiti dinamici HMC

Il pannello **HMC** visualizza l'elenco di indirizzi IP delle HMC rilevate dalla serie di ambiti dinamici. I vari pannelli di credenziali, come **Credenziali AIX**, elencano le credenziali configurate nella serie di ambiti.

Aggiunta degli ambiti dinamici HMC

Per aggiungere una serie di ambiti dinamici HMC, specificare l'indirizzo IP di una singola HMC insieme a una singola credenziale per l'accesso alla HMC. Facoltativamente, è possibile specificare le credenziali per AIX, Linux e VIOS per consentire il rilevamento delle LPAR degli IBM Power System gestiti dalla HMC. Una volta creata la serie di ambiti dinamici HMC, è possibile modificarla per definire ulteriori indirizzi IP HMC. È possibile modificare le serie di ambiti dinamici HMC anche per supportare più credenziali per l'accesso alle HMC e alle LPAR.

Informazioni su questa attività

Per aggiungere una serie di ambiti, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Per definire una nuova serie di ambiti dinamici HMC, fare clic su **Aggiungi nuovo ambito dinamico HMC**.
Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**.

HMC Dynamic Scope Set

Asterisks (*) indicate mandatory fields that are required to complete this action.

Describe Scope Set
Enter a name for the HMC scope set.

Scope set name: *

Enter Host Name or IP Address of HMC
IP address: *

Enter Access Information for HMC
Enter Computer System specific access information.

Credential name: *

Authentication type: *
 Password
 PKI

User Name: *

Password *

Confirm password *

Test Credential

LPARs
Select which types of LPARs to include in the dynamic discovery.

Select LPAR types:
 AIX
 Linux
 VIOS

Enter Access Information for AIX LPARs
Enter Computer System specific access information.

Credential name: *

Authentication type: *
 Password
 PKI

User Name: *

Password *

Confirm password *

Test access credentials for AIX LPARs
Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Enter Access Information for Linux LPARs
Enter Computer System specific access information.

Credential name: *

Authentication type: *
 Password
 PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux LPARs
Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Enter Access Information for VIOS LPARs
Enter Computer System specific access information.

Credential name: *

Authentication type: *
 Password
 PKI

User Name: *

Password *

Confirm password *

Test access credentials for VIOS LPARs
Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Save Cancel

Figura 45. Aggiungere serie di ambiti dinamici HMC

3. Nel pannello **Descrivi serie di ambiti**, immettere un nome univoco nel campo **Nome serie di ambiti**.
4. Nel pannello **Immettere il nome host o l'indirizzo IP dell'HMC**, immettere il nome host o l'indirizzo IP dell'HMC.

5. Nel pannello **Immettere le informazioni di accesso per l'HMC**, immettere i seguenti dettagli -
 - a) Immettere il **Nome credenziale**
 - b) Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
 - c) Immettere il **Nome utente** utilizzato per autenticarsi con la HMC.
 - d) Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
 - e) Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.
 - f) Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica sull'HMC.
 - g) Opzionale: Fare clic su **Verifica credenziali** per verificare le credenziali dell'HMC di destinazione.
6. Nel pannello **LPAR**, selezionare quali tipi di LPAR (AIX, LINUX, VIOS) includere nel rilevamento dinamico.
7. Se si seleziona uno dei tipi di LPAR (AIX, Linux, VIOS), immettere le relative informazioni di accesso.

Enter Access Information for Linux LPARs

Enter Computer System specific access information.

Credential name: *

Authentication type: *

Password

PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux LPARs

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the HMC Dynamic Scope Set definition.

IP address:

Test Credential

Figura 46. Esempio: Immettere le informazioni di accesso per le LPAR Linux

- a) Immettere il **Nome credenziale**.
- b) Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
- c) Immettere il **Nome utente** utilizzato per autenticarsi con la rispettiva LPAR.
- d) Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
- e) Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.

- f) Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica su ogni LPAR.
 - g) Opzionale: Immettere l'**indirizzo IP** di una LPAR gestita da questa HMC e fare clic su **Verifica credenziale** per verificare le credenziali dell'LPAR di destinazione.
8. Fare clic su **Salva** per salvare la serie di ambiti dinamici HMC.

Modifica degli ambiti dinamici HMC - Indirizzi IP HMC

È possibile modificare l'elenco di indirizzi IP HMC associati a una serie di ambiti dinamici HMC esistente.

Informazioni su questa attività

Per modificare l'elenco di indirizzi IP HMC, attenersi a questa procedura.

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
 2. Per modificare la serie di ambiti, fare clic sull'icona .
Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**.
 - Per aggiungere un indirizzo IP HMC alla serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **HMC**, fare clic su **Aggiungi HMC**. Verrà visualizzata la pagina **Ambiti dinamici HMC**.
 - b. Immettere l'**Indirizzo IP** dell'HMC nel pannello **Descrivi indirizzo o host**.
 - c. Fare clic su **Salva** per aggiungere l'HMC.
 - Per modificare un indirizzo IP HMC nella serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **HMC**, fare clic sull'icona . Verrà visualizzata la pagina **Ambiti dinamici HMC**.
 - b. Modificare l'**Indirizzo IP** dell'HMC nel pannello **Descrivi indirizzo o host**.
 - c. Fare clic su **Salva** per modificare l'HMC.
 - Per eliminare un indirizzo IP HMC nella serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **HMC**, fare clic sull'icona .
 - b. Nella finestra di dialogo, fare clic su **OK** per confermare l'eliminazione.
- Nota:** Una serie di ambiti dinamici HMC deve sempre avere almeno un indirizzo IP HMC definito. TSA non consente l'eliminazione di tutti gli indirizzi IP HMC.

Modifica degli ambiti dinamici HMC - Credenziali

È possibile modificare l'elenco di credenziali associate a una serie di ambiti dinamici HMC esistente.

Informazioni su questa attività

Una serie di ambiti dinamici HMC deve sempre avere almeno una credenziale HMC definita. TSA non consente l'eliminazione di tutte le credenziali HMC. Se non esistono credenziali per AIX, Linux o VIOS, TSA non raccoglie informazioni dettagliate per quel tipo di LPAR.

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Per modificare la serie di ambiti, fare clic sull'icona .
Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**.
 - Per aggiungere una credenziale per HMC, AIX, Linux o VIOS, HMC, attenersi a questa procedura:

- a. Nel pannello **Credenziali** appropriato, fare clic su **Aggiungi credenziali**. Ad esempio, per aggiungere una credenziale HMC, fare clic su **Aggiungi credenziali HMC** nel pannello **Credenziali HMC**. Viene visualizzata la pagina **Nuove credenziali di rilevamento HMC**.
 - b. Immettere il **Nome credenziale**
 - c. Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
 - d. Immettere il **Nome utente** utilizzato per autenticarsi con la HMC o la rispettiva LPAR.
 - e. Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
 - f. Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.
 - g. Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica sulle HMC o sulle LPAR.
 - h. **Facoltativo:** immettere l'**indirizzo IP** dell'HMC o dell'LPAR e fare clic su **Verifica credenziali** per verificare le credenziali dell'LPAR di destinazione.
 - i. Fare clic su **Salva** per salvare le credenziali della serie di ambiti dinamici HMC.
- Per modificare una credenziale per HMC, AIX, Linux o VIOS, attenersi a questa procedura:
 - a. Nel pannello **Credenziali** appropriato, fare clic sull'icona  accanto alla credenziale che si desidera modificare. Ad esempio, per modificare una credenziale HMC, fare clic su  nel pannello **Credenziali HMC** per la credenziale da modificare. Viene visualizzata la pagina **Modifica credenziali di rilevamento HMC**.
 - b. Nel pannello **Immetti informazioni di accesso**, è possibile modificare i seguenti dettagli -
 - 1) Immettere il **Nome utente** utilizzato per autenticarsi con la HMC o la rispettiva LPAR.
 - 2) Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
 - 3) Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
 - 4) Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.
 - 5) Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica su ogni HMC e su ogni LPAR.
 - c. **Facoltativo:** immettere l'**indirizzo IP** dell'HMC o dell'LPAR e fare clic su **Verifica credenziali** per verificare le credenziali dell'LPAR di destinazione.
 - d. Fare clic su **Salva** per aggiornare le modifiche per la rispettiva credenziale.
 - Per eliminare una credenziale per HMC, AIX, Linux o VIOS, attenersi a questa procedura:
 - a. Nel pannello **Credenziali** appropriato, fare clic sull'icona **Elimina**  per la rispettiva credenziale. Ad esempio, per eliminare una credenziale HMC, fare clic sull'icona  nel pannello **Credenziali HMC** per la credenziale da eliminare. Verrà visualizzato un messaggio di conferma.
 - b. Fare clic su **OK** per eliminare la credenziale.
 - Per modificare una credenziale per HMC, AIX, Linux o VIOS, attenersi a questa procedura:

- a. Se esistono più credenziali per HMC, AIX, Linux o VIOS, è possibile modificare l'ordine delle credenziali per le HMC o l'LPAR. Quando esiste una sola credenziale, le frecce verso l'alto e verso il basso non appaiono nella colonna **Azioni** per il pannello delle credenziali.
- b. Nel pannello **Credenziali** appropriato, fare clic sull'icona  o  per riordinare le credenziali.

Abilitazione o disabilitazione delle serie di ambiti dinamici

È possibile abilitare o disabilitare una serie di ambiti dinamici HMC.

Informazioni su questa attività

Una serie di ambiti disabilitata viene ignorata durante un rilevamento pianificato.

Nota: Un rilevamento manuale può sempre essere eseguito, indipendentemente dallo stato della serie di ambiti.

Disabilitazione delle serie di ambiti dinamici

Procedura

Per disabilitare una serie di ambiti dinamici HMC, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Fare clic sull'icona **Abilita**  accanto alla serie di ambiti che si desidera disabilitare.

Abilitazione delle serie di ambiti dinamici

Procedura

Per abilitare una serie di ambiti dinamici HMC, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Fare clic sull'icona **Disabilita**  accanto alla serie di ambiti che si desidera abilitare.

Rilevamento di una HMC

È possibile avviare manualmente un rilevamento di una singola HMC in una serie di ambiti dinamici HMC. Il rilevamento raccoglie le informazioni sull'HMC insieme alle LPAR associate.

Procedura

Per avviare manualmente un rilevamento di un'HMC, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Fare clic sull'icona  per la serie di ambiti dinamici HMC richiesta. Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**.
3. Fare clic sull'icona  accanto all'indirizzo IP HMC che si desidera rilevare.

Rilevamento delle serie di ambiti dinamici

È possibile avviare manualmente un rilevamento per una serie di ambiti dinamici HMC. Il rilevamento raccoglie le informazioni su tutte le HMC definite per la serie di ambiti insieme alle LPAR associate.

Procedura

Per avviare manualmente un rilevamento per una serie di ambiti dinamici HMC, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici HMC**.

Verrà visualizzata la pagina **Ambiti dinamici HMC**.

2. Fare clic sull'icona **Esegui**  accanto alla serie di ambiti che si desidera rilevare.

Eliminazione degli ambiti dinamici HMC

È possibile eliminare una serie di ambiti dinamici HMC esistente.

Procedura

Per eliminare una serie di ambiti dinamici HMC, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti dinamici HMC**.
Verrà visualizzata la pagina **Ambiti dinamici HMC**.
2. Fare clic sull'icona **Elimina**  accanto alla serie di ambiti che si desidera eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare la serie di ambiti dinamici HMC.

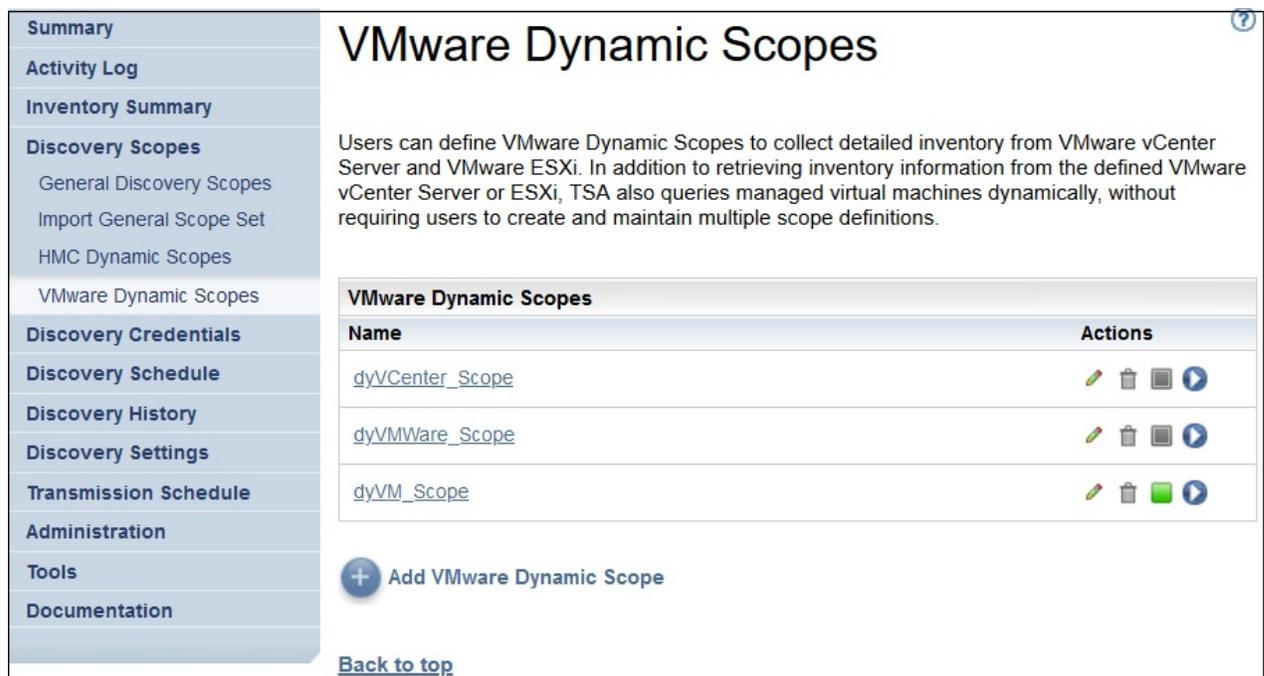
Nota: Quando si conferma l'eliminazione della serie di ambiti dinamici HMC, vengono eliminate anche le rispettive informazioni di accesso per LPAR AIX, Linux o VIOS.

Ambiti dinamici VMware

È possibile definire ambiti dinamici VMware per raccogliere inventari dettagliati dalle istanze VMware vCenter Server e ESXi. Gli ambiti dinamici VMware raccolgono anche informazioni sui server x86 gestiti dall'istanza VMware vCenter Server o ESXi e le macchine virtuali Linux e Windows su quei sistemi.

TSA richiama le informazioni di inventario dalle istanze VMware vCenter Server e ESXi definite. TSA interroga anche le macchine virtuali gestite dalle istanze VMware dinamicamente, senza la necessità di creare e gestire più definizioni di ambito. È necessario definire un ambito per le istanze VMware e selezionare i tipi di Macchina virtuale (Linux e Windows) che si desidera siano automaticamente scansionate quando vengono rilevate queste istanze VMware. Il vantaggio è che, anche se le macchine virtuali cambiano, non è necessario riconfigurare TSA.

Il rilevamento VMware vCenter Server trova tutte le istanza VMware ESXi che gestisce, eliminando così la necessità di rilevare le istanze VMware ESXi direttamente. Le istanze VMware ESXi non gestite da un VMware vCenter Server, possono essere direttamente rilevate da TSA definendo VMware ESXi nell'ambito dinamico VMware.



VMware Dynamic Scopes	
Name	Actions
dyVCenter_Scope	  
dyVMWare_Scope	  
dyVM_Scope	  

Figura 47. Ambiti dinamici VMware

Visualizzazione di ambiti dinamici VMware, serie di ambiti e credenziali

È possibile visualizzare gli ambiti dinamici VMware e le serie di ambiti esistenti.

Informazioni su questa attività

Per visualizzare le serie di ambiti dinamici VMware esistenti, fare clic su **Ambiti di rilevamento > Ambiti dinamici VMware** nel pannello di navigazione. Verrà visualizzata la pagina **Ambiti dinamici VMware**. Il pannello **Ambiti dinamici VMware** contiene un elenco di ambiti dinamici VMware.

Per visualizzare gli ambiti e le credenziali associati a una specifica serie di ambiti dinamici, fare clic sul nome della serie di ambiti nella colonna **Nome**. Verrà visualizzata la pagina **Serie di ambiti dinamici VMware**.

VMware Dynamic Scope Set

General

Name: dyVCenter_Scope

VMware vCenter Server / ESXi

Type	Value	Actions
Address	9.5.80.130	

Add VMware vCenter Server or ESXi

VMware Credentials

Credential name	User Name	Actions
dyVCenter_Cred	administrator@tsa.local	

Add VMware Credentials

Linux Credentials

Credential name	Type	User Name	Actions
-----------------	------	-----------	---------

Add Linux Credentials

No credentials have been defined

Windows Credentials

Credential name	User Name	Actions
-----------------	-----------	---------

Add Windows Credentials

No credentials have been defined

Figura 48. Visualizzare una serie di ambiti dinamici VMware

Il pannello **VMware vCenter Server/ESXi** visualizza l'elenco di indirizzi IP delle istanze VMware vCenter Server e ESXi rilevate dalla serie di ambiti dinamici. I vari pannelli di credenziali, come **Credenziali Linux**, elencano le credenziali configurate nella serie di ambiti.

Aggiunta degli ambiti dinamici VMware

Per aggiungere una serie di ambiti dinamici VMware, specificare l'indirizzo IP di una singola istanza di VMware vCenter Server o ESXi insieme a una singola credenziale per l'accesso all'istanza VMware. Facoltativamente, è possibile specificare le credenziali per Linux e Windows per consentire il rilevamento delle macchine virtuali dei server x86 gestiti dall'istanza VMware. Una volta creata la serie di ambiti dinamici VMware, è possibile modificarla per definire ulteriori indirizzi IP VMware vCenter Server o ESXi. È possibile modificare le serie di ambiti dinamici VMware anche per supportare più credenziali per l'accesso all'istanza VMware e alle macchine virtuali.

Informazioni su questa attività

Per aggiungere una serie di ambiti dinamici VMware, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Per definire una nuova serie di ambiti dinamici VMware, fare clic su **Aggiungi nuovo ambito dinamico VMware**.
Verrà visualizzata la pagina **Serie di ambiti dinamici VMware**.

VMware Dynamic Scope Set

Asterisks (*) indicate mandatory fields that are required to complete this action.

Describe Scope Set
Enter a name for the VMware scope set.
Scope set name: *

Enter Host Name or IP Address of VMware vCenter Server or ESXi
IP address: *

Enter Access Information for VMware
Enter Computer System specific access information.
Credential name: *
User Name: *
Password: *
Confirm password: *

Virtual Machines
Select which types of virtual machines to include in the dynamic discovery.
Select virtual machine types: Linux Windows

Enter Access Information for Linux virtual machines
Enter Computer System specific access information.
Credential name: *
Authentication type: * Password PKI
User Name: *
Password *
Confirm password *

Test access credentials for Linux virtual machines
Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.
IP address:

Enter Access Information for Windows virtual machines
Enter Computer System specific access information.
Credential name: *
User Name: *
Password: *
Confirm password: *

Test access credentials for Windows virtual machines
Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.
IP address:

Figura 49. Visualizzare una serie di ambiti dinamici VMware

3. Nel pannello **Descrivi serie di ambiti**, immettere un nome univoco nel campo **Nome serie di ambiti**.
4. Nel pannello **Immettere il nome host o l'indirizzo IP di VMware vCenter Server o ESXi**, immettere il nome host o l'indirizzo IP dell'istanza VMware vCenter Server o ESXi.
5. Nel pannello **Immettere le informazioni di accesso per VMware**, immettere i seguenti dettagli -
 - a) Immettere il **Nome credenziale**
 - b) Immettere il **Nome utente** utilizzato per autenticarsi all'istanza VMware vCenter Server o ESXi
 - c) Compilare i campi **Password** e **Conferma password**

- d) Opzionale: Fare clic su **Verifica credenziali** per verificare le credenziali dell'istanza VMware vCenter Server o ESXi di destinazione.
6. Nel pannello **Macchine virtuali**, selezionare la macchina virtuale (Linux, Windows) da includere nel rilevamento dinamico.
7. Se si seleziona una macchina virtuale Linux, immettere le rispettive informazioni di accesso.

Enter Access Information for Linux virtual machines

Enter Computer System specific access information.

Credential name: *

Authentication type: *

Password

PKI

User Name: *

Password *

Confirm password *

Test access credentials for Linux virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address:

[Test Credential](#)

Figura 50. Immettere le informazioni di accesso per la macchina virtuale Linux

- a) Immettere il **Nome credenziale**.
- b) Selezionare il **Tipo di autenticazione**
- **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
- c) Immettere il **Nome utente** utilizzato per autenticarsi con la rispettiva macchina virtuale.
- d) Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
- e) Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.
- f) Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica su ogni macchina virtuale.
- g) Opzionale: Immettere l'**Indirizzo IP** della macchina virtuale e fare clic su **Verifica credenziali** per verificare le credenziali della macchina virtuale di destinazione.
8. Se si seleziona una macchina virtuale Windows, immettere le rispettive informazioni di accesso.

Figura 51. Immettere le informazioni di accesso per la macchina virtuale Windows

- a) Immettere il **Nome credenziale**.
 - b) Immettere il **Nome utente** utilizzato per autenticarsi con la rispettiva macchina virtuale.
 - c) Compilare i campi **Password** e **Conferma password**.
 - d) Opzionale: Immettere l'**Indirizzo IP** della macchina virtuale e fare clic su **Verifica credenziali** per verificare le credenziali della macchina virtuale di destinazione.
9. Fare clic su **Salva** per salvare la serie di ambiti dinamici VMware.

Modifica degli ambiti dinamici VMware - Indirizzi IP VMware vCenter Server o ESXi

È possibile modificare l'elenco di indirizzi IP VMware vCenter Server o ESXi associati a una serie di ambiti dinamici VMware esistente.

Informazioni su questa attività

Per modificare l'elenco di indirizzi IP VMware vCenter Server o ESXi, attenersi a questa procedura.

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Per modificare la serie di ambiti, fare clic sull'icona .
Verrà visualizzata la pagina **Serie di ambiti dinamici VMware**.
 - Per aggiungere un indirizzo IP VMware vCenter Server o ESXi alla serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **VMware vCenter Server/ESXi**, fare clic su **Aggiungi VMware vCenter Server o ESXi**. Verrà visualizzata la pagina **Ambiti dinamici VMware**.
 - b. Immettere l'**Indirizzo IP** di VMware vCenter Server o ESXi nel pannello **Descrivi indirizzo o host**.
 - c. Fare clic su **Salva** per aggiungere l'istanza VMware vCenter Server o ESXi.
 - Per modificare un indirizzo IP VMware vCenter Server o ESXi nella serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **VMware vCenter Server/ESXi**, fare clic sull'icona . Verrà visualizzata la pagina **Ambiti dinamici VMware**.
 - b. Modificare l'**Indirizzo IP** dell'istanza VMware vCenter Server o ESXi nel pannello **Descrivi indirizzo o host**.

- c. Fare clic su **Salva**.
- Per eliminare un indirizzo IP VMware vCenter Server o ESXi nella serie di ambiti, attenersi a questa procedura:
 - a. Nel pannello **VMware vCenter Server/ESXi**, fare clic sull'icona .
 - b. Nella finestra di dialogo, fare clic su **OK** per confermare l'eliminazione.

Nota: Una serie di ambiti dinamici VMware deve sempre avere almeno un indirizzo IP VMware vCenter Server o ESXi definito. TSA non consente l'eliminazione di tutti gli indirizzi IP VMware.

Modifica degli ambiti dinamici VMware - Credenziali

È possibile modificare l'elenco di credenziali associate a una serie di ambiti dinamici VMware esistente.

Informazioni su questa attività

Una serie di ambiti dinamici VMware deve sempre avere almeno una credenziale VMware definita. TSA non consente l'eliminazione di tutte le credenziali VMware. Se non esistono credenziali per Linux o Windows, TSA non raccoglie informazioni dettagliate relativamente a quel tipo di macchina virtuale.

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Per modificare la serie di ambiti, fare clic sull'icona  .
Verrà visualizzata la pagina **Serie di ambiti dinamici VMware**.
 - Per aggiungere una credenziale per VMware o Windows, attenersi a questa procedura:
 - a. Nel pannello **Credenziali** appropriato, fare clic su **Aggiungi credenziali**. Ad esempio, per aggiungere una credenziale VMware, fare clic su **Aggiungi credenziali VMware** nel pannello **Credenziali VMWare**. Viene visualizzata la pagina **Nuove credenziali di rilevamento VMware**.
 - b. Immettere il **Nome credenziale**
 - c. Immettere il **Nome utente** utilizzato per l'autenticazione nelle istanze di VMware vCenter Server o ESXi oppure nelle macchine virtuali Windows.
 - d. Compilare i campi **Password** e **Conferma password**.
 - e. **Facoltativo:** Immettere l'**indirizzo IP** dell'istanza di VMware vCenter Server o ESXi oppure della macchina virtuale Windows e fare clic su **Verifica credenziale** per verificare le credenziali della destinazione.
 - f. Fare clic su **Salva** per salvare la rispettiva credenziale.
 - Per aggiungere una credenziale per Linux, attenersi a questa procedura:
 - a. Nel pannello **Credenziali Linux**, fare clic su **Aggiungi credenziali Linux**. Viene visualizzata la pagina **Nuove credenziali di rilevamento VMware**.
 - b. Immettere il **Nome credenziale**
 - c. Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
 - d. Immettere il **Nome utente** utilizzato per l'autenticazione nelle macchine virtuali Linux.
 - e. Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
 - f. Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.

- g. Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica sulle macchine virtuali Linux.
- h. **Facoltativo:** immettere l'**Indirizzo IP** della macchina virtuale Linux e fare clic su **Verifica credenziali** per verificare le credenziali della macchina virtuale Linux di destinazione.
- i. Fare clic su **Salva** per salvare la credenziale Linux.
- Per modificare una credenziale per VMware o Windows, attenersi a questa procedura:
 - a. Nel pannello **Credenziali** appropriato, fare clic sull'icona  accanto alla credenziale che si desidera modificare. Ad esempio, per modificare una credenziale VMware, fare clic su  nel pannello **Credenziali VMware** per la credenziale da modificare. Viene visualizzata la pagina **Modifica credenziali di rilevamento VMware**.
 - b. Nel pannello **Immetti informazioni di accesso**, è possibile modificare i seguenti dettagli -
 - 1) Immettere il **Nome utente** utilizzato per autenticarsi quando ci si connette alle istanze di VMware vCenter Server o ESXi o alle macchine virtuali Windows.
 - 2) Compilare i campi **Password** e **Conferma password**.
 - c. **Facoltativo:** Immettere l'**indirizzo IP** dell'istanza di VMware vCenter Server o ESXi oppure della macchina virtuale Windows e fare clic su **Verifica credenziale** per verificare le credenziali della destinazione.
 - d. Fare clic su **Salva** per aggiornare le modifiche per la rispettiva credenziale.
- Per modificare una credenziale per Linux, attenersi a questa procedura:
 - a. Nel pannello **Credenziali Linux**, fare clic sull'icona  accanto alla credenziale che si desidera modificare. Viene visualizzata la pagina **Modifica credenziali di rilevamento VMware**.
 - b. Nel pannello **Immetti informazioni di accesso**, è possibile modificare i seguenti dettagli -
 - 1) Selezionare il **Tipo di autenticazione**
 - **Password** - Utilizza la password fornita.
 - **PKI** - Utilizza la chiave SSH associata alla serie di ambiti specifica.
 - 2) Immettere il **Nome utente** utilizzato per l'autenticazione nella macchina virtuale Linux.
 - 3) Quando **Tipo di autenticazione** corrisponde a **Password**, compilare i campi **Password** e **Conferma password**.
 - 4) Quando **Tipo di autenticazione** corrisponde a **PKI**, compilare i campi **Passphrase** e **Conferma passphrase**, se la chiave SSH è crittografata. Se la chiave SSH non è crittografata, lasciare vuoti questi due campi.
 - 5) Se **Tipo di autenticazione** corrisponde a **PKI**, fare clic su **Scegli file** e caricare la chiave privata in TSA. È necessario distribuire esternamente la chiave pubblica sulle macchine virtuali Linux.
 - 6) **Facoltativo:** immettere l'**Indirizzo IP** della macchina virtuale e fare clic su **Verifica credenziali** per verificare le credenziali della macchina virtuale Linux di destinazione.
 - c. Fare clic su **Salva** per aggiornare le modifiche per la rispettiva credenziale.
- Per eliminare una credenziale per VMware, Linux o Windows, attenersi a questa procedura:
 - a. Nel pannello **Credenziali** appropriato, fare clic sull'icona **Elimina**  per la rispettiva credenziale. Ad esempio, per eliminare una credenziale VMware, fare clic sull'icona  nel pannello **Credenziali VMware** per la credenziale da eliminare. Verrà visualizzato un messaggio di conferma.
 - b. Fare clic su **OK** per eliminare la credenziale.
- Per modificare l'ordine di una credenziale per VMware, Linux o Windows, attenersi a questa procedura:

- a. Se esistono più credenziali per VMware, Linux o Windows, è possibile modificare l'ordine delle credenziali per i VMware o le macchine virtuali. Quando esiste una sola credenziale, le frecce verso l'alto e verso il basso non appaiono nella colonna **Azioni** per il pannello delle credenziali.
- b. Nel pannello **Credenziali** appropriato, fare clic sull'icona  o  per riordinare le credenziali.

Abilitazione o disabilitazione delle serie di ambiti dinamici

È possibile abilitare o disabilitare una serie di ambiti dinamici VMware.

Informazioni su questa attività

Una serie di ambiti disabilitata viene ignorata durante un rilevamento pianificato.

Nota: Un rilevamento manuale può sempre essere eseguito, indipendentemente dallo stato della serie di ambiti.

Disabilitazione delle serie di ambiti dinamici

Procedura

Per disabilitare una serie di ambiti dinamici VMware, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Fare clic sull'icona **Abilita**  accanto alla serie di ambiti che si desidera disabilitare.

Abilitazione delle serie di ambiti dinamici

Procedura

Per abilitare una serie di ambiti dinamici VMware, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Fare clic sull'icona **Disabilita**  accanto alla serie di ambiti che si desidera abilitare.

Rilevamento di un VMware vCenter o ESXi

È possibile avviare manualmente un rilevamento di un singolo VMware vCenter Server o ESXi in una serie di ambiti dinamici VMware. Il rilevamento raccoglie le informazioni sull'istanza VMware insieme alle macchine virtuali associate.

Procedura

Per avviare manualmente un rilevamento di un VMware vCenter Server o ESXi, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Fare clic sull'icona  per la serie di ambiti dinamici VMware richiesta. Verrà visualizzata la pagina **Serie di ambiti dinamici VMware**.
3. Fare clic sull'icona  accanto all'indirizzo IP del VMware vCenter Server o ESXi che si desidera rilevare.

Rilevamento delle serie di ambiti dinamici

È possibile avviare manualmente un rilevamento per una serie di ambiti dinamici VMware. Il rilevamento raccoglie le informazioni su tutte le istanze VMware vCenter Server o ESXi definite per la serie di ambiti insieme alle macchine virtuali associate.

Procedura

Per avviare manualmente un rilevamento per una serie di ambiti dinamici VMware, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Fare clic sull'icona **Esegui**  accanto alla serie di ambiti che si desidera rilevare.

Eliminazione degli ambiti dinamici VMware

È possibile eliminare una serie di ambiti dinamici VMware esistente.

Procedura

Per eliminare una serie di ambiti dinamici VMware, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti dinamici VMware**.
Verrà visualizzata la pagina **Ambiti dinamici VMware**.
2. Fare clic sull'icona **Elimina**  accanto alla serie di ambiti che si desidera eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare la serie di ambiti dinamici VMware.

Nota: Quando si conferma l'eliminazione della serie di ambiti dinamici VMware, vengono eliminate anche le rispettive informazioni di accesso per le macchine virtuali Linux o Windows.

Ambiti di rilevamento generali

Il processo di rilevamento cerca gli elementi IT nell'infrastruttura. Un ambito di rilevamento definisce un singolo indirizzo IP o intervallo rilevato durante il processo di rilevamento. Gli ambiti di rilevamento sono raggruppati in serie di ambiti denominate dall'utente.

Visualizzazione di ambiti di rilevamento e serie di ambiti

È possibile visualizzare gli ambiti di rilevamento e le serie di ambiti esistenti.

Informazioni su questa attività

Per visualizzare le serie di ambiti di rilevamento esistenti, fare clic su **Ambiti di rilevamento > Ambiti di rilevamento generali** nel pannello di navigazione. Verrà visualizzata la pagina **Ambiti di rilevamento generali**. Il pannello **Ambiti di rilevamento generali** contiene un elenco di serie di ambiti.

Per visualizzare gli ambiti contenuti in una serie di ambiti, fare clic sulla serie di ambiti. Verrà visualizzata la pagina **Serie di ambiti di rilevamento**.

- Il pannello **Generali** visualizza il nome della serie di ambiti.
- Il pannello **Conteggio indirizzi IP** visualizza il numero totale di indirizzi IP nella specifica serie di ambiti.
- Il pannello **Ambiti** visualizza i dettagli sugli ambiti nella serie di ambiti.

Aggiunta degli abiti di rilevamento

È possibile aggiungere una serie di ambiti e un nuovo ambito a tale serie, aggiungere un ambito a una serie di ambiti esistenti o spostare ambiti in altre serie di ambiti. Per aggiungere un ambito, specificare un indirizzo IP valido, un intervallo di indirizzi IP, una rete o una subnet.

Informazioni su questa attività

Suggerimenti: Esistono alcune considerazioni pratiche per la configurazione degli ambiti di rilevamento e delle serie di ambiti.

- Più indirizzi IP ci sono nell'ambito di rilevamento e più tempo impiega il rilevamento. È possibile modificare la dimensione del rilevamento disabilitando o abilitando le serie di ambiti o escludendo indirizzi IP, intervalli di indirizzi IP, reti o subnet da un ambito in una serie di ambiti.

Per ridurre al minimo il tempo impiegato da un rilevamento, configurare gli ambiti di rilevamento in modo che considerino solo gli elementi che si vogliono rilevare e disabilitare le serie di ambiti o escludere indirizzi IP, intervalli di indirizzi IP, reti o subnet che non si desidera o non è necessario rilevare.

Nota: Per prestazioni ottimali, limitare il numero totale di indirizzi IP in una serie di ambiti a 400 o meno. Per informazioni su come importare una serie di ambiti, consultare la sezione [“Importazione di una serie di ambiti”](#) a pagina 73

- Non tutti gli elementi sono uguali. Ad esempio, un router con decine di interfacce può impiegare un tempo più lungo di un singolo host per un rilevamento completo.
- Se si utilizza l'autenticazione PKI per il rilevamento del dispositivo, è possibile associare una sola chiave SSH a ciascuna serie di ambiti.

Per ulteriori informazioni sulle procedure ottimali per configurare gli ambiti di rilevamento, fare riferimento alla Guida dell'assistente alla configurazione TSA.

Per aggiungere una serie di ambiti e un ambito, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
2. Per definire una nuova serie di ambiti di rilevamento, fare clic su **Aggiungi nuova serie di ambiti**.
Verrà visualizzata la pagina **Serie di ambiti di rilevamento**.

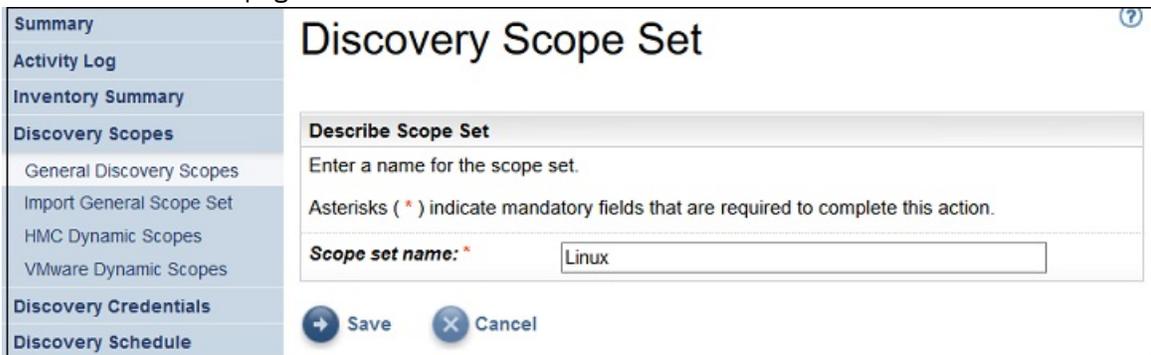


Figura 52. Serie di ambiti di rilevamento

- a) Immettere un nome di serie di ambiti univoco nel campo **Nome serie di ambiti**
- b) Fare clic su **Salva**.

La nuova serie di ambiti viene creata e viene visualizzata la pagina **Ambiti di rilevamento generali**.

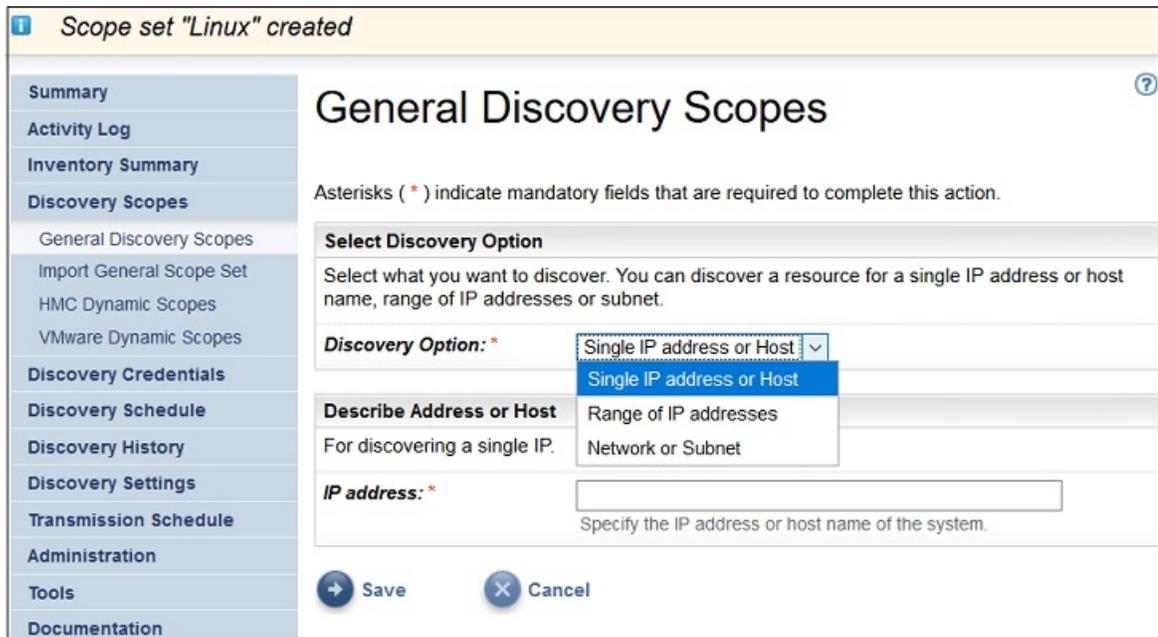


Figura 53. Ambiti di rilevamento generali

3. Specificare una delle seguenti opzioni nel pannello **Seleziona opzione di rilevamento**:

- Host o indirizzo IP singolo

Per **Descrivi indirizzo o host**, immettere l'indirizzo IP o il nome host.

- Intervallo di indirizzi IP

Per **Descrivi intervallo indirizzi**, immettere l'indirizzo IP iniziale, l'indirizzo IP finale e, facoltativamente, una descrizione negli appositi campi.

- Rete o subnet

Per **Descrivi rete o subnet**, immettere l'indirizzo IP, la mask e, facoltativamente, una descrizione negli appositi campi.

4. Se si vogliono escludere dal rilevamento host, indirizzi IP, intervalli di indirizzi IP o subnet, fare clic su **Aggiungi esclusione** e attenersi a questa procedura:

- a) Selezionare **Host**, **Intervallo** o **Subnet**.

- b) Specificare l'indirizzo IP, l'intervallo di indirizzi IP o la subnet che si desidera escludere dal rilevamento.

- c) Opzionale: Specificare una descrizione per l'indirizzo IP, l'intervallo di indirizzi IP o la subnet che si ha intenzione di escludere dal rilevamento.

Nota: Le esclusioni sono applicabili solo ad un ambito definito con un intervallo di indirizzi IP o una subnet.

Nota: È possibile riutilizzare un indirizzo IP, un intervallo di indirizzi IP, subnet o una descrizione in qualsiasi ambito o esclusione in una serie di ambiti.

- d) Per aggiungere ulteriori esclusioni, fare clic su **Aggiungi esclusione** e attenersi alla procedura precedentemente descritta per definire ulteriori esclusioni.

5. Fare clic su **Salva** per salvare l'ambito e le esclusioni. Verrà visualizzata la pagina **Serie di ambiti di rilevamento** con il nuovo ambito incluso nell'elenco.

6. Per aggiungere più ambiti a questa serie di ambiti, fare clic su **Aggiungi nuovo ambito** e seguire la procedura precedente per definire altri ambiti.

Nota: Per prestazioni ottimali, limitare il numero totale di indirizzi IP in una serie di ambiti a 400 o meno.

Aggiunta di un ambito di rilevamento a una serie di ambiti esistente

È possibile aggiungere un ambito a una serie di ambiti esistente.

Procedura

Per aggiungere un ambito a una serie di ambiti esistente, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
2. Nel pannello **Ambiti di rilevamento generali**, selezionare la serie di ambiti a cui si desidera aggiungere un ambito.
Verrà visualizzata la pagina **Serie di ambiti di rilevamento**.
3. Fare clic su **Aggiungi nuovo ambito**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
4. Nel pannello **Seleziona opzione di rilevamento**, specificare una delle seguenti opzioni.
 - Host o indirizzo IP singolo
Per **Descrivi indirizzo o host**, immettere l'indirizzo IP o il nome host.
 - Intervallo di indirizzi IP
Per **Descrivi intervallo indirizzi**, immettere l'indirizzo IP iniziale, l'indirizzo IP finale e, facoltativamente, una descrizione negli appositi campi.
 - Rete o subnet
Per **Descrivi rete o subnet**, immettere l'indirizzo IP, la mask e, facoltativamente, una descrizione negli appositi campi.
5. Se si vogliono escludere dal rilevamento host, indirizzi IP, intervalli di indirizzi IP o subnet, fare clic su **Aggiungi esclusione** e attenersi a questa procedura:
 - a) Selezionare **Host**, **Intervallo** o **Subnet**.
 - b) Specificare l'indirizzo IP, l'intervallo di indirizzi IP o la subnet che si desidera escludere dal rilevamento.
 - c) Opzionale: Specificare una descrizione per l'indirizzo IP, l'intervallo di indirizzi IP o la subnet che si ha intenzione di escludere dal rilevamento.
Nota: Le esclusioni sono applicabili solo ad un ambito definito con un intervallo di indirizzi IP o una subnet.
Nota: È possibile riutilizzare un indirizzo IP, un intervallo di indirizzi IP, subnet o una descrizione in qualsiasi ambito o esclusione in una serie di ambiti.
 - d) Per aggiungere ulteriori esclusioni, fare clic su **Aggiungi esclusione** e attenersi alla procedura precedentemente descritta per definire ulteriori esclusioni.
6. Fare clic su **Salva** per salvare l'ambito e le esclusioni.
Verrà visualizzata la pagina **Serie di ambiti di rilevamento** con il nuovo ambito incluso nell'elenco.

Modifica di una serie di ambiti di rilevamento

È possibile modificare una serie di ambiti di rilevamento esistente modificando le impostazioni per la serie di ambiti.

Informazioni su questa attività

Per modificare una serie di ambiti di rilevamento esistente, seguire questa procedura.

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
2. Per modificare la serie di ambiti, fare clic sull'icona **Modifica**  accanto alla serie di ambiti.

Verrà visualizzata la pagina **Serie di ambiti di rilevamento**. È possibile modificare la serie di ambiti modificando un ambito, aggiungendo un ambito, spostando un ambito in un'altra serie di ambiti o eliminando un ambito.

- Per aggiungere un ambito, attenersi a questa procedura:
 - a. Fare clic su **Aggiungi nuovo ambito**.
 - b. Nel pannello **Seleziona opzione di rilevamento**, specificare una delle seguenti opzioni:
 - Host/indirizzo IP singolo
Per **Descrivi indirizzo o host**, immettere l'indirizzo IP o il nome host.
 - Intervallo di indirizzi IP
Per **Descrivi intervallo indirizzi**, immettere l'indirizzo IP iniziale, l'indirizzo IP finale e, facoltativamente, una descrizione negli appositi campi.
 - Rete o subnet
Per **Descrivi rete o subnet**, immettere l'indirizzo IP, la mask e, facoltativamente, una descrizione negli appositi campi.
 - c. Se si vogliono escludere dal rilevamento host, indirizzi IP o subnet, fare clic su **Aggiungi esclusione** e attenersi a questa procedura:
 - 1) Selezionare **Host, Intervallo** o **Subnet**.
 - 2) Specificare l'indirizzo IP, l'intervallo di indirizzi IP o la subnet che si desidera escludere dal rilevamento.
 - 3) Per aggiungere ulteriori esclusioni, fare clic su **Aggiungi esclusione** e attenersi alla procedura precedentemente descritta per definire ulteriori esclusioni.
 - d. Fare clic su **Salva** per salvare l'ambito e le esclusioni. Verrà visualizzata la pagina **Serie di ambiti di rilevamento** con il nuovo ambito incluso nell'elenco.
- Per spostare un ambito in un'altra serie di ambiti, attenersi a questa procedura:
 - a. Fare clic su **Sposta ambiti**.
 - b. Sulla pagina **Sposta gli ambiti da una serie a un'altra**, selezionare gli ambiti che si desidera spostare dall'elenco **Ambiti**.
 - c. Selezionare la serie di ambiti dall'elenco **Serie di ambiti destinazione** in cui si desidera spostare gli ambiti.
 - d. Fare clic su **Sposta**.
- Per modificare un ambito, attenersi a questa procedura:
 - a. Fare clic sull'icona **Modifica**  per un ambito specifico.
 - b. È possibile modificare **Opzione di rilevamento, Indirizzi IP, Esclusioni**, ecc.
 - c. Fare clic su **Salva** per salvare l'ambito e le esclusioni. Verrà visualizzata la pagina **Serie di ambiti di rilevamento** con il nuovo ambito incluso nell'elenco.
- Per eliminare un ambito, attenersi a questa procedura:
 - a. Fare clic sull'icona **Elimina**  accanto all'ambito che si desidera eliminare.
 - b. Fare clic su **OK** per confermare che si desidera eliminare l'ambito di rilevamento.

Eliminazione degli ambiti di rilevamento

È possibile eliminare ambiti di rilevamento esistenti all'interno di una serie di ambiti o intere serie di ambiti.

Informazioni su questa attività

Procedura

Per eliminare un ambito di rilevamento, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
2. Modificare la serie di ambiti che contiene l'ambito di rilevamento che si desidera eliminare facendo clic sull'icona **Modifica**  accanto alla serie di ambiti.
Verrà visualizzata la pagina **Serie di ambiti di rilevamento**.
3. Fare clic sull'icona **Elimina**  accanto all'ambito che si desidera eliminare.
4. Fare clic su **OK** per confermare che si desidera eliminare l'ambito di rilevamento.

Eliminazione delle serie di ambiti di rilevamento

È possibile eliminare le serie di ambiti di rilevamento esistenti.

Procedura

Nota: Prima di poter eliminare una serie di ambiti, è necessario eliminare tutte le credenziali associate alla serie di ambiti.

Per eliminare una serie di ambiti di rilevamento, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.
Verrà visualizzata la pagina **Ambiti di rilevamento generali**.
2. Fare clic sull'icona **Elimina**  accanto alla serie di ambiti che si desidera eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare la serie di ambiti di rilevamento.

Importazione di una serie di ambiti

È possibile importare un elenco di indirizzi IP per definire una nuova serie di ambiti.

Informazioni su questa attività

Una nuova serie di ambiti viene creata in base al nome specificato e l'elenco degli indirizzi IP dal file di input. TSA effettua le seguenti convalide quando si importa una serie di ambiti:

- Controlla se il nome della serie di ambiti esiste già.
- Verifica ogni riga del file per controllare se è un indirizzo IP valido o meno.
- Ignora gli spazi iniziali e finali quando convalida l'indirizzo IP.
- Ignora gli indirizzi IP duplicati.

Procedura

Per importare gli indirizzi IP, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Importa serie di ambiti generali**.
Viene visualizzata la pagina **Importa serie di ambiti generali**.
2. Immettere il **Nuovo nome serie di ambiti**.

Nota: Immettere un nome univoco che non sia utilizzato da alcuna serie di ambiti esistente. Se viene immesso un nome di serie di ambiti esistente, si riceve un messaggio - Nome serie di ambiti già esistente.

3. Fare clic su **Scegli file** per selezionare il file di testo.

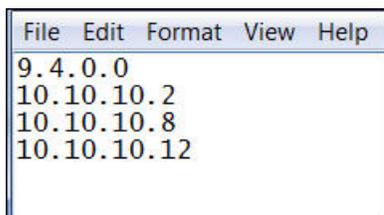


Figura 54. Importa serie di ambiti

Nota: Il file di testo deve essere formato da una singola colonna, dove ogni riga contiene un singolo indirizzo IP e nessun altro dato.

4. Fare clic su **Importa file serie di ambiti** per importare la serie di ambiti. Viene visualizzato un messaggio di stato quando l'importazione viene completata correttamente - **Serie di ambiti importata correttamente.**

Nota: Se il file della serie di ambiti ha più di 400 indirizzi IP, si riceve il messaggio di avvertenza - **Serie di ambiti importata correttamente. Ma il numero di elementi ambito va oltre i limiti consigliati, per prestazioni ottimali mantenersi entro i 400.**

5. Dopo aver importato la serie di ambiti è possibile modificarla nella sezione **Ambiti di rilevamento generali** dell'interfaccia utente e associare le credenziali nella sezione **Credenziali di rilevamento.**

Impostazioni di rilevamento

Utilizzare la pagina **Impostazioni di rilevamento** per regolare le impostazioni di rilevamento avanzate.

Configurazione delle impostazioni di connessione

Utilizzare la pagina **Impostazioni di connessione** per configurare il Rilevamento SLP e rilevare i dispositivi di storage EMC tramite i provider SMI-S EMC.

Informazioni su questa attività

Per impostazione predefinita, un lavoro di rilevamento tenta di trovare i provider SMI-S EMC eseguendo una query SLP per determinare l'indirizzo IP e la porta. Se SLP non è disponibile nella rete (ad esempio se ci sono politiche di sicurezza che bloccano i messaggi SLP), il rilevamento dei dispositivi di storage EMC può ancora essere effettuato disabilitando il Rilevamento SLP e configurando le porte su cui il provider SMI-S EMC ascolta le richieste di query.

Procedura

1. Selezionare le opzioni **Abilita** o **Disabilita** per abilitare o disabilitare il Rilevamento SLP.

Nota: Per impostazione predefinita, il rilevamento SLP è abilitato.

2. Se si disabilita il rilevamento SLP, è necessario impostare una o più porte di connessione del provider EMC SMI-S -
 - a) **Porte EMC SMI-S HTTPS:** 5989 è la porta HTTPS predefinita su cui il provider SMI-S EMC ascolta le richieste di query. Se si specificano più porte, separarle con le virgole. EMC SMI-S ascolta su queste porte le richieste di connessione (ad esempio da TSA). TSA deve conoscere la porta per iniziare la connessione.
 - b) **Porte EMC SMI-S HTTP:** 5988 è la porta HTTP predefinita su cui il provider SMI-S EMC ascolta le richieste di query. TSA tenta prima una connessione HTTPS (se configurata) e, se non riesce, tenta la connessione tramite le porte HTTP definite. Se si desidera evitare le connessioni HTTP, non definire porte HTTP. Se si specificano più porte HTTP, separarle con virgole. EMC SMI-S ascolta su queste porte le richieste di connessione (ad esempio da TSA). TSA deve conoscere la porta per iniziare la connessione.

3. Fare clic su **Salva** per salvare le impostazioni di connessione. Si riceve un messaggio - *Le impostazioni di connessione del rilevamento sono state salvate correttamente.*

Credenziali di rilevamento

Le credenziali di rilevamento includono nomi utente, password o chiavi SSH e stringhe di community SNMP (Simple Network Management Protocol) che TSA utilizza per accedere a risorse configurate in **Ambiti di rilevamento generali** durante il rilevamento.

Visualizzazione delle credenziali

Il processo di rilevamento richiede delle credenziali, come gli ID utente e le password, per accedere alle risorse.

Informazioni su questa attività

Importante: Le informazioni di accesso specificate devono corrispondere alle informazioni di accesso per la risorsa di destinazione di rilevamento. Se si modificano le informazioni di accesso, come una password, sulla risorsa di destinazione, assicurarsi di modificare anche le informazioni di accesso a Technical Support Appliance associate.

È possibile visualizzare le credenziali esistenti facendo clic su **Credenziali di rilevamento** nel pannello di navigazione. Viene visualizzata la pagina **Credenziali di rilevamento**.

Name	Type	User Name	Password Changed Date	Scope Set Restriction	Actions
IFS 840	Computer System	JVlaz	6/15/15	IFS 840	
IFS 820	Computer System	user	6/15/15	IFS 820	
Windows 2012 R2	Computer System (Windows)	Administrator	6/16/15	Windows 2012 R2	

[Add New Credentials](#)

[Back to top](#)

Figura 55. Nuove credenziali di rilevamento

Visualizzazione dei dettagli delle credenziali

È possibile visualizzare informazioni dettagliate su una specifica credenziale di rilevamento.

Informazioni su questa attività

Per visualizzare i dettagli della credenziale, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Credenziali di rilevamento**.
Viene visualizzata la pagina **Credenziali di rilevamento** con tutte le credenziali esistenti elencate.
2. Per visualizzare i dettagli per una credenziale specifica, fare clic sul nome della credenziale.
Viene visualizzata la pagina **Credenziali di rilevamento** con le informazioni sulla credenziale selezionata.

Discovery Credentials

General	
Name:	AIX_Cred
Type:	HostAuth
User name:	root
Scope set:	AIX_Scope

Properties	
Name	Value
name	AIX_Cred
authtype	Default
username	root
order	1

[Go back](#) [Edit Credential](#)

Figura 56. Dettagli credenziali di rilevamento

Attività correlate

Modifica delle credenziali

È possibile modificare credenziali esistenti per fornire il controllo dell'accesso per il processo di rilevamento.

Aggiunta di credenziali

Aggiungere le credenziali per fornire il controllo dell'accesso per il processo di rilevamento.

Informazioni su questa attività

Per aggiungere le credenziali, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Credenziali di rilevamento**.
Viene visualizzata la pagina **Credenziali di rilevamento**.
2. Per creare una credenziale, fare clic su **Aggiungi nuove credenziali**.
Viene visualizzata la pagina **Nuove credenziali di rilevamento**.

- Summary
- Activity Log
- Inventory Summary
- Discovery Scopes
- Discovery Credentials
- Discovery Schedule
- Discovery History
- Discovery Settings
- Transmission Schedule
- Administration
- Tools
- Documentation

New Discovery Credentials ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Name

Define an identifying name for the credential.

Name: *

Select Credential

Select the type of credential you want to define.

Credential Type: *

Enter Access Information

Enter Computer System specific access information.

User name: *

Password

Confirm password

Authentication type:

Select Scope Set Restriction

Select whether to use the access information across all defined discovery scopes or to restrict application of this access information to a given scope.

Select: *

Restrict To Selected Scope Set

Identifies the scope set this credential is restricted to.

Scope set name: *

Test access credentials

Specify the hostname or IP address against which you want to test the access credentials. This hostname or IP address information is not mandatory to save the discovery credentials.

Hostname or IP address:

Figura 57. Nuove credenziali di rilevamento

- a) Nel campo **Nome**, immettere un nome identificativo per la credenziale.
- b) Nell'elenco a discesa **Tipo di credenziale**, selezionare il tipo di credenziale da creare.
- c) Nel pannello **Immetti informazioni di accesso**, specificare le informazioni per il tipo di credenziale selezionato:

Le informazioni richieste dipendono dal tipo di credenziale. Per dettagli sulle informazioni di accesso necessarie per ogni tipo di credenziale, consultare [“Requisiti di software e credenziale per l'ambiente di rilevamento”](#) a pagina 6.

Importante: Le informazioni di accesso specificate devono corrispondere alle informazioni di accesso per la risorsa di destinazione di rilevamento. Se si modificano le informazioni di accesso

per la risorsa di destinazione, assicurarsi di modificare anche le informazioni di accesso a TSA associate. Per maggiori informazioni, fare riferimento alla Guida dell'assistente alla configurazione di IBM Technical Support Appliance.

Suggerimento: La pagina **Credenziali di rilevamento** visualizza l'ultima volta che è stata modificata la password. Se si modifica regolarmente la password sulla risorsa di destinazione, è possibile utilizzare questa informazione per assicurarsi di modificare anche la password su TSA in modo che corrisponda alla nuova password per la risorsa di destinazione. Per informazioni sulla visualizzazione delle credenziali di rilevamento, consultare [“Visualizzazione delle credenziali”](#) a pagina 75.

- d) Il pannello **Seleziona limitazione serie di ambiti** viene utilizzato per specificare se una credenziale è limitata ad una singola serie di ambiti oppure si applica a tutte le serie di ambiti. Se **Tipo di credenziale** è **Computer** e il **Tipo di autenticazione** è **PKI**, questo pannello non verrà visualizzato. Le credenziali PKI devono essere sempre inserite in una singola serie di ambiti.

Suggerimento: Creare credenziali di rilevamento limitate a una specifica serie di ambiti può migliorare le prestazioni poiché riduce il numero di credenziali da tentare per le risorse da rilevare.

- e) Il pannello **Limita alla serie di ambiti selezionata** viene utilizzata per limitare una credenziale a una singola serie di ambiti. Questo pannello è visibile in una delle due seguenti condizioni:

- Nel pannello **Seleziona limitazione della serie di ambiti** è selezionato **Limita informazioni di accesso ad un ambito specificato** oppure
- Il **Tipo di credenziali** è **Computer** e il **Tipo di autenticazione** è **PKI**.

La credenziale è utilizzata solo per rilevare la serie di ambiti selezionata. Quando si effettua il rilevamento con una serie di ambiti differente, la credenziale non viene utilizzata. Questo metodo impedisce tentativi di accesso non validi che possono provocare il blocco dell'account.

- f) Se il tipo di credenziale è **Computer**, **Computer (Windows)**, **SNMP**, o **SNMPV3**, è possibile verificare se le credenziali sono corrette. La funzione **Verifica** per il tipo di credenziale **Computer** supporta i seguenti dispositivi:

- Dispositivi che utilizzano autenticazione basata su SSH o Telnet.
- XIV
- DS6000 & DS8000
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON / VNX / VMAX tramite EMC SMI-S
- IBM TS3100 / TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4500
- IBM TS7700
- IBM DS3000, DS4000 e DS5000 se protetto da password
- Windows
- Palo Alto Networks (PAN-OS)

Per verificare le credenziali, immettere un indirizzo IP o nome host per il dispositivo di destinazione rispetto al quale si desidera verificare le credenziali e fare clic su **Verifica**.

Nota:

- Il nome host immesso non deve contenere caratteri di sottolineatura ("_").
- Per eseguire il rilevamento o verificare la credenziale su sistemi che utilizzano sistemi operativi Linux, AIX, IBM i, o HP-UX, abilitare SSH.

- g) Fare clic su **Salva**.

La nuova credenziale viene visualizzata nella pagina **Credenziali di rilevamento**.

Nota: Si consiglia di eseguire il backup della configurazione TSA quando si creano o si modificano le credenziali di rilevamento.

3. Per modificare l'ordine in cui TSA utilizza una credenziale per accedere a una risorsa, fare clic sull'icona **Freccia su**  o sull'icona **Freccia giù**  accanto alla credenziale da spostare su o giù nell'elenco.

Per informazioni su come viene utilizzato l'ordine, consultare [“Credenziali di rilevamento”](#) a pagina 2.

Viene nuovamente visualizzata la pagina con l'elenco di **Credenziali di rilevamento** con il nuovo ordine.

Modifica delle credenziali

È possibile modificare credenziali esistenti per fornire il controllo dell'accesso per il processo di rilevamento.

Informazioni su questa attività

Per modificare le credenziali, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Credenziali di rilevamento**.

Viene visualizzata la pagina **Credenziali di rilevamento** con tutte le credenziali esistenti elencate.

2. Modificare la credenziale facendo clic sull'icona **Modifica**  accanto alla credenziale.

Viene visualizzata la pagina **Modifica credenziali di rilevamento**.

- a) Nel pannello **Modifica informazioni di accesso**, è possibile modificare le informazioni di accesso per questa credenziale.

Importante: Le informazioni di accesso specificate devono corrispondere alle informazioni di accesso per la risorsa di destinazione di rilevamento. Se si modificano le informazioni di accesso per la risorsa di destinazione, assicurarsi di modificare anche le informazioni di accesso a TSA associate. Per maggiori informazioni, fare riferimento alla Guida dell'assistente alla configurazione di IBM Technical Support Appliance.

Suggerimento: La pagina **Credenziali di rilevamento** visualizza l'ultima volta che è stata modificata la password. Se si modifica regolarmente la password sulla risorsa di destinazione, è possibile utilizzare questa informazione per assicurarsi di modificare anche la password su TSA in modo che corrisponda alla nuova password per la risorsa di destinazione. Per informazioni sulla visualizzazione delle credenziali di rilevamento, consultare [“Visualizzazione delle credenziali”](#) a pagina 75.

- b) Il pannello **Seleziona limitazione serie di ambiti** viene utilizzato per specificare se una credenziale è limitata ad una singola serie di ambiti oppure si applica a tutte le serie di ambiti. Se il **Tipo di credenziale** è **Computer** e il **Tipo di autenticazione** è **PKI**, questo pannello non verrà visualizzato. Le credenziali PKI devono essere sempre inserite in una singola serie di ambiti.

Suggerimento: Creare credenziali di rilevamento limitate a una specifica serie di ambiti può migliorare le prestazioni poiché riduce il numero di credenziali da tentare per le risorse da rilevare.

- c) Il pannello **Limita alla serie di ambiti selezionata** viene utilizzata per limitare una credenziale a una singola serie di ambiti. Questo pannello è visibile in una delle due seguenti condizioni:

- Nel pannello **Seleziona limitazione della serie di ambiti** è selezionato **Limita informazioni di accesso ad un ambito specificato** oppure
- Il **Tipo di credenziali** è **Computer** e il **Tipo di autenticazione** è **PKI**.

La credenziale viene utilizzata solo quando si rileva la serie di ambiti selezionata. Questa credenziale non viene utilizzata con altre serie di ambiti. Questo metodo impedisce tentativi di accesso non validi che possono provocare il blocco dell'account.

d) Se il tipo di credenziale è **Computer**, **Computer (Windows)**, **SNMP**, o **SNMPV3**, è possibile verificare se le credenziali sono corrette. Per verificare queste credenziali, immettere un indirizzo IP o nome host per la destinazione rispetto alla quale si desidera verificare le credenziali e fare clic su **Verifica**.

Nota: Il nome host immesso non deve contenere caratteri di sottolineatura ("_").

e) Fare clic su **Salva**.

La credenziale modificata viene visualizzata nella pagina **Credenziali di rilevamento**.

3. Per modificare l'ordine di priorità con cui TSA utilizzata una credenziale per accedere a una risorsa, fare clic sull'icona **Freccia su**  o sull'icona **Freccia giù**  accanto alla credenziale da spostare su o giù nell'elenco.

Per informazioni su come viene utilizzato l'ordine, consultare [“Credenziali di rilevamento” a pagina 2](#).

Viene nuovamente visualizzata la pagina con l'elenco di **Credenziali di rilevamento** con il nuovo ordine.

Concetti correlati

Credenziali di rilevamento

Le credenziali di rilevamento sono una raccolta di nomi utente, password o chiavi SSH e stringhe di community SNMP (Simple Network Management Protocol) utilizzate da TSA per accedere alle risorse durante il rilevamento.

Requisiti di software e credenziale per l'ambiente di rilevamento

Per poter effettuare il rilevamento di endpoint o risorse nell'ambiente, TSA deve avere accesso a tali risorse. Si consiglia di creare un account di servizio su ciascuna risorsa che è specificamente per TSA, da utilizzare durante l'accesso a tale risorsa.

Eliminazione delle credenziali

È possibile eliminare le credenziali che TSA utilizza quando accede alle risorse.

Informazioni su questa attività

Per eliminare una credenziale, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Credenziali di rilevamento**.
Viene visualizzata la pagina **Credenziali di rilevamento**.
2. Fare clic sull'icona **Elimina**  accanto alla credenziale da eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare la credenziale.

Pianificazione rilevamento

I rilevamenti sono pianificati per garantire che i dati rilevati siano sempre attuali e accurati. È possibile visualizzare la pianificazione del rilevamento e i dettagli degli ultimi rilevamenti, modificare le pianificazioni del rilevamento e disabilitare i rilevamenti pianificati. È anche possibile eseguire un rilevamento in qualsiasi momento.

Prima di iniziare

Per impostazione predefinita, TSA utilizza la pianificazione Rilevamento completo per rilevare tutti gli elementi IT definiti in ambiti dinamici HMC e VMware, oltre che in ambiti di rilevamento generali. TSA automaticamente estende il rilevamento di elementi IT durante il processo di rilevamento, per ridurre al minimo l'impatto.

Un'alternativa consiste nel creare varie pianificazioni definite dall'utente. Questo consente di estendere il rilevamento di ambiti di rilevamento specifici a date e ore differenti, quando l'impatto per la rete e gli

elementi IT è minimo (o ideale). In questo caso, la pianificazione di rilevamento completo dovrebbe essere disabilitata in favore di pianificazioni definite dall'utente.

All'inizio di qualsiasi rilevamento pianificato, l'appliance esegue il lavoro di manutenzione pre-rilevamento durante il quale non sono disponibili alcune operazioni come Riepilogo inventario, Ambiti di rilevamento, Pianificazione rilevamento e Credenziali. Durante il lavoro di manutenzione pre-rilevamento lo stato di

Discovery Manager sul pannello **Riepilogo** è impostato sul simbolo di avvertenza (⚠). Inoltre, viene visualizzato un messaggio di avvertenza sui pannelli TSA che indica che alcune funzioni sono temporaneamente non disponibili: Come parte della manutenzione pre-rilevamento, Discovery Manager è temporaneamente offline. Alcune funzioni della IU correlate al rilevamento o all'inventario possono visualizzare informazioni parziali o non visualizzare informazioni durante questo intervallo (generalmente fino a 10 minuti).

Quando la manutenzione pre-rilevamento termina correttamente, lo stato di **Discovery Manager** torna ad essere OK(✅) nella pagina **Riepilogo** e riprende l'attività di rilevamento completo (entro 10 minuti).

Visualizzazione della pianificazione di rilevamento

È possibile visualizzare le informazioni di riepilogo su una pianificazione di rilevamento.

Informazioni su questa attività

Per visualizzare la pianificazione del rilevamento, attenersi a questa procedura:

Procedura

Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**.

Viene visualizzata la pagina **Pianificazione rilevamento**.

Il pannello **Pianifica** visualizza il nome della pianificazione, la successiva esecuzione pianificata, la pianificazione dell'esecuzione e le azioni (Modifica (✏), Elimina (🗑), Abilita/Disabilita (🟢/🟡), Esegui (▶) per ogni pianificazione.

Fare clic sull'icona ▶ per visualizzare tutte le serie di ambiti assegnate per la pianificazione. Per la pianificazione di un rilevamento completo, l'icona elenca tutte le serie di ambiti definite in TSA e che sono assegnate alla pianificazione per impostazione predefinita.

The screenshot shows the 'Discovery Schedule' page. On the left is a navigation menu with items like Summary, Activity Log, Inventory Summary, Discovery Scopes, Discovery Credentials, Discovery Schedule (selected), Discovery History, Discovery Settings, Transmission Schedule, Administration, Tools, and Documentation. The main content area has a title 'Discovery Schedule' and a warning message: 'As part of Pre-Discovery Maintenance (automatically performed at the beginning of a Discovery), some functions such as Inventory Summary, Discovery Scopes and Credentials will be unavailable. Please ensure the Discovery Manager status is depicted by a green check mark icon in the Summary screen before resuming activity (typically up to 10 minutes)'. Below this is a table for the 'Schedule' with columns: Name, Next run, Runs at, and Actions. It lists 'Full Discovery' and 'AIX Schedule'. At the bottom, there is a 'History' table with columns: Status, Schedule Name, Instance, State, and Comments. The history shows a completed 'Full Discovery' on 11/3/17.

Name	Next run:	Runs at	Actions
▶ Full Discovery	11/10/17 8:20 AM GMT	08:20 AM on Friday	✏ 🟢 ▶
▶ AIX Schedule	11/7/17 4:20 AM GMT	04:20 AM on Tuesday	✏ 🗑 🟢 ▶

Status	Schedule Name	Instance	State	Comments
✅	Full Discovery	11/3/17 8:20 AM GMT	Complete	<ul style="list-style-type: none">Last status: OKLast run: 11/3/17 8:20 AM GMTLast completed: 11/3/17 8:33 AM GMTLast duration: 13 mins,42 secsInitiator: System

Figura 58. Pianificazione rilevamento

Nota: Se TSA è stato appena installato, migrato o aggiornato all'ultima versione, il nuovo TSA ha una pianificazione di rilevamento denominata **Rilevamento completo**, creata con la data predefinita (Martedì ore 2:15). La pianificazione Rilevamento completo può essere modificata o disabilitata, ma non può essere eliminata. Se si hanno pianificazioni di rilevamento pre-definite (abilitate/disabilitate), gli stessi valori sono ripristinati dopo la migrazione.

Il pannello **Cronologia** visualizza lo stato, il nome pianificazione e ulteriori dettagli dei lavori di rilevamento correntemente in esecuzione e precedenti.

Aggiunta della pianificazione di rilevamento

È possibile aggiungere nuove pianificazioni affinché il processo di rilevamento sia eseguito a un'ora specifica. Le nuove pianificazioni consentono a TSA di rilevare un sottoinsieme degli elementi IT nella data e ora specificate.

Procedura

1. Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**.
Viene visualizzata la pagina **Pianificazione rilevamento**.
2. Fare clic su **Aggiungi pianificazione rilevamento**. Viene visualizzata la pagina **Aggiungi pianificazione rilevamento**.

Add Discovery Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Discovery Schedule

Enter the name for this schedule and select the Scope Sets to create a periodic discovery.

Schedule Name: *

Scope Sets: Show only unassigned Scope Sets

Select Scope Sets: *

BNT_Scope

HMC_Scope

HPOBA_Scope

Schedule

Select when you want the discovery performed.

At hour: *

At minute: *

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Figura 59. Aggiungi pianificazione rilevamento

3. Nel campo **Nome pianificazione**, immettere un nome identificativo per la pianificazione.
4. Selezionare l'opzione **Mostra solo serie di ambiti non assegnati** per visualizzare solo le serie di ambiti non assegnati ad altre pianificazione di rilevamento definite dall'utente.
5. Selezionare le serie di ambiti desiderate dall'elenco **Seleziona serie di ambiti**.
È possibile utilizzare **Seleziona tutto/Deseleziona tutto** per selezionare tutte o nessuna serie di ambiti.
6. Utilizzare gli elenchi **A ore** e **A minuti** per selezionare il nuovo orario.
7. Selezionare **Modalità di selezione giorno**.

Per giorno settimanale (dom-sab)

Per pianificare il rilevamento in giorni specifici di una settimana, selezionare l'opzione **Per giorno settimanale (dom-sab)**.

Schedule

Select when you want the discovery performed.

At hour: *

At minute: *

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Figura 60. Per giorno settimanale (dom-sab)

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni della settimana.

Per data mensile (1-31)

Per pianificare il rilevamento in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni del mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

8. Fare clic su **Salva**.

Viene visualizzata di nuovo la pagina **Pianificazione rilevamento** con la nuova pianificazione.

Modifica della pianificazione di rilevamento

TSA fornisce una pianificazione predefinita in base alla quale eseguire il processo di rilevamento a un determinato orario. È possibile modificare la pianificazione predefinita oppure utilizzare pianificazioni personalizzate in base alle proprie esigenze.

Informazioni su questa attività

Procedura

1. Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**.

Viene visualizzata la pagina **Pianificazione rilevamento**.

2. Fare clic su **Modifica pianificazione** (icona ).

Viene visualizzata la pagina **Modifica pianificazione rilevamento**.

a) Modificare **Nome pianificazione**, **Serie di ambiti** e **Seleziona serie di ambiti** come necessario nel pannello **Pianificazione rilevamento**.

Nota: È possibile modificare questi campi per il rilevamento completo predefinito.

b) Modificare **A ore**, **A minuti**, **Modalità di selezione giorno** e **Nei giorni** come necessario nel pannello **Pianifica**.

3. Fare clic su **Salva**.

Viene visualizzata di nuovo la pagina **Pianificazione rilevamento** con la pianificazione modificata.

Disabilitazione della pianificazione di rilevamento

È possibile disabilitare i rilevamenti pianificati.

Prima di iniziare

Nota: Se sono state configurate pianificazioni rilevamento definite dall'utente, si consiglia di disabilitare la pianificazione **Rilevamento completo**, per evitare che si verifichino rilevamenti duplicati degli stessi elementi IT.

Procedura

Per disabilitare i rilevamenti pianificati, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**.
Viene visualizzata la pagina **Pianificazione rilevamento**.
2. Fare clic su  /  per la rispettiva pianificazione per disabilitare/abilitare la pianificazione del rilevamento.

Eliminazione della pianificazione di rilevamento

È possibile eliminare i rilevamenti pianificati.

Procedura

Per eliminare i rilevamenti pianificati, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**.
Viene visualizzata la pagina **Pianificazione rilevamento**.
2. Fare clic sull'icona  per la rispettiva pianificazione da eliminare.

Nota: Non è possibile eliminare la pianificazione di rilevamento completo predefinita, ma può essere disabilitata, se necessario.

Viene visualizzato un messaggio per confermare l'eliminazione della pianificazione di rilevamento selezionata.

3. Fare clic su **OK** per eliminare la pianificazione.

Esecuzione del rilevamento

È possibile eseguire un rilevamento su richiesta, invece che attendere il successivo rilevamento pianificato. È possibile eseguire un rilevamento su tutti gli ambiti di rilevamento definiti, una pianificazione di rilevamento specifica, o su serie di ambiti o ambiti di rilevamento specifici.

Procedura

Per eseguire un rilevamento su tutti gli ambiti definiti, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Pianificazione rilevamento**. Viene visualizzata la pagina **Pianificazione rilevamento**.
2. Fare clic su **Esegui ora il rilevamento completo**. La sezione Cronologia viene aggiornata per indicare che il rilevamento è in esecuzione.

Nota: TSA tenta di minimizzare gli impatti sull'ambiente di rete. Come risultato, il processo di rilevamento adotta un approccio iterativo e misurato, per cui un rilevamento completo può richiedere fino a 72 ore. È possibile monitorare il processo di rilevamento nella sezione **Riepilogo lavori** sulla pagina **Riepilogo**.

3. Per eseguire un rilevamento su un ambito specifico, fare clic sull'icona **Esegui**  per tale ambito.
4. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo**

lavori, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Esecuzione del rilevamento su serie di ambiti generali

Procedura

Per eseguire il rilevamento su una serie di ambiti specifica, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti di rilevamento generali**.

Verrà visualizzata la pagina **Ambiti di rilevamento generali**. Questa pagina visualizza un elenco di tutte le serie di ambiti definite per questo TSA.

Name	Actions
Brocade_Scope	[edit] [delete] [refresh] [execute]
HMC_Scope	[edit] [delete] [refresh] [execute]
Import	[edit] [delete] [refresh] [execute]
Juniper_Scope	[edit] [delete] [refresh] [execute]
Linux	[edit] [delete] [refresh] [execute]
NSeries_Scopeset	[edit] [delete] [refresh] [execute]
PT_Scope	[edit] [delete] [refresh] [execute]
TS3500_Scope	[edit] [delete] [refresh] [execute]
Test_IPRange_ScopeSet	[edit] [delete] [refresh] [execute]

Figura 61. Eseguire il rilevamento su ambiti specifici

2. Per eseguire un rilevamento su una serie di ambiti specifica, fare clic sull'icona **Esegui**  per tale serie di ambiti.
3. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Esecuzione del rilevamento su serie di ambiti dinamici HMC

Procedura

Per eseguire il rilevamento su una serie di ambiti specifica, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento** > **Ambiti dinamici HMC**.

Verrà visualizzata la pagina **Ambiti dinamici HMC**. Questa pagina visualizza un elenco di tutte le serie di ambiti definite per questo TSA.

Figura 62. Ambiti dinamici HMC

2. Per eseguire un rilevamento su una serie di ambiti specifica, fare clic sull'icona **Esegui** per tale serie di ambiti.
3. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Esecuzione del rilevamento su serie di ambiti VMWare

Procedura

Per eseguire il rilevamento su una serie di ambiti specifica, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Serie di ambiti dinamici VMWare**. Verrà visualizzata la pagina **Ambiti dinamici VMWare**. Questa pagina visualizza un elenco di tutte le serie di ambiti definite per questo TSA.

Figura 63. Eseguire il rilevamento su ambiti dinamici VMWare

2. Per eseguire un rilevamento su una serie di ambiti specifica, fare clic sull'icona **Esegui** per tale serie di ambiti.

3. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

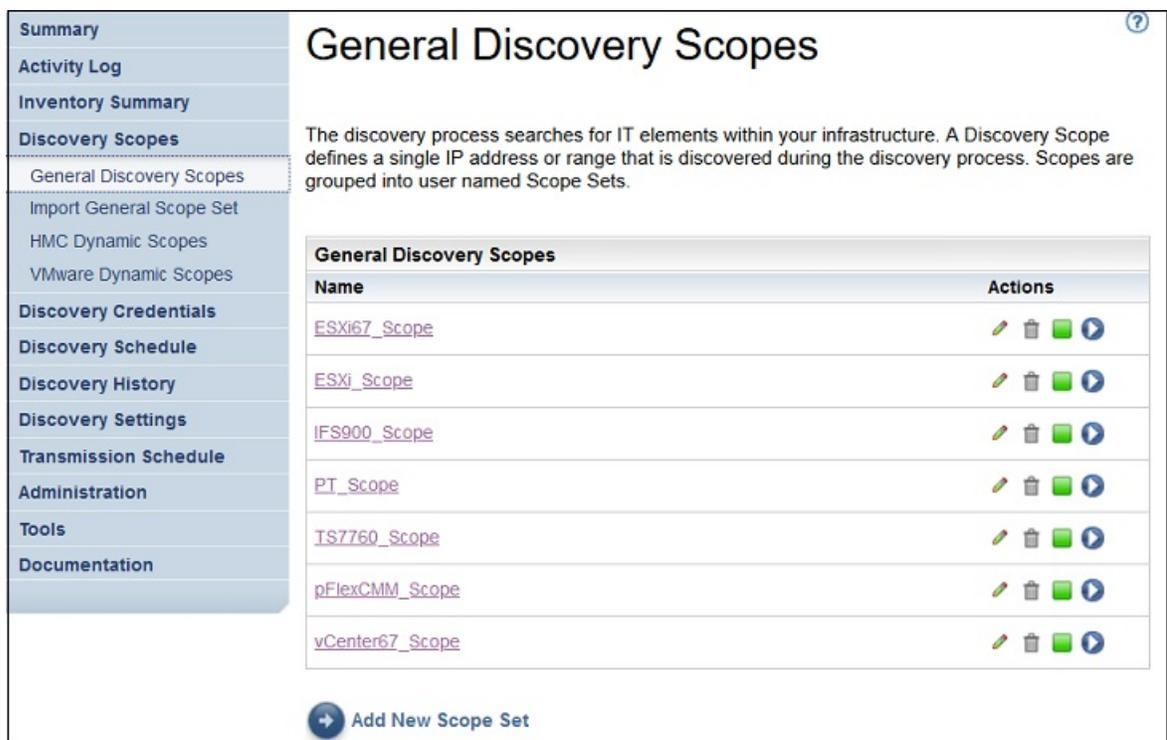
Esecuzione del rilevamento su ambiti

È possibile eseguire un rilevamento su richiesta, invece che attendere il successivo rilevamento pianificato. È possibile eseguire un rilevamento su tutti gli ambiti di rilevamento definiti, una pianificazione di rilevamento specifica, o su serie di ambiti o ambiti di rilevamento specifici.

Esecuzione del rilevamento su ambiti generali

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti di rilevamento generali**. Verrà visualizzata la pagina **Ambiti di rilevamento generali**.



General Discovery Scopes

The discovery process searches for IT elements within your infrastructure. A Discovery Scope defines a single IP address or range that is discovered during the discovery process. Scopes are grouped into user named Scope Sets.

Name	Actions
ESXi67_Scope	   
ESXi_Scope	   
IFS900_Scope	   
PT_Scope	   
TS7760_Scope	   
pFlexCMM_Scope	   
vCenter67_Scope	   

 Add New Scope Set

Figura 64. Ambiti di rilevamento

2. Fare clic sulla serie di ambiti che contiene l'ambito da rilevare. Verrà visualizzata la pagina **Serie di ambiti di rilevamento**. Questa pagina mostra tutti gli ambiti definiti per tale serie di ambiti.

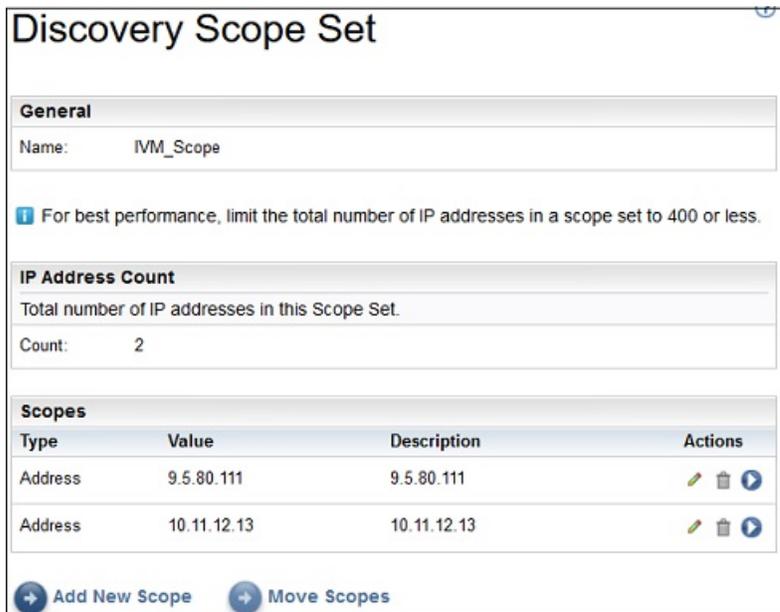


Figura 65. Eseguire il rilevamento su ambiti specifici

3. Per eseguire un rilevamento su un ambito specifico, fare clic sull'icona **Esegui** per tale ambito.
4. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Esecuzione del rilevamento su ambiti dinamici HMC

Procedura

1. Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici HMC**. Verrà visualizzata la pagina **Ambiti dinamici HMC**.

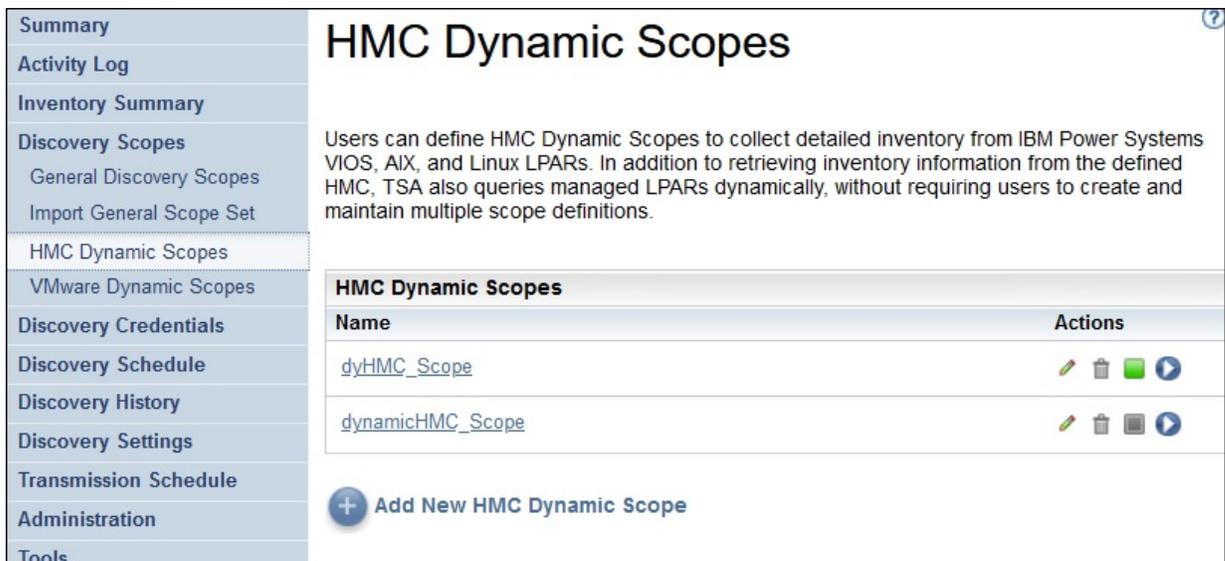


Figura 66. Ambiti dinamici HMC

2. Fare clic sulla serie di ambiti che contiene l'ambito da rilevare.
Verrà visualizzata la pagina **Serie di ambiti dinamici HMC**. Questa pagina mostra tutti gli ambiti definiti per tale serie di ambiti.

Summary	<h1>HMC Dynamic Scope Set</h1>						
Activity Log							
Inventory Summary							
Discovery Scopes							
General Discovery Scopes							
Import General Scope Set							
HMC Dynamic Scopes							
VMware Dynamic Scopes							
Discovery Credentials							
Discovery Schedule							
Discovery History							
Discovery Settings							
	General						
	Name: dyHMC_Scope						
	HMC						
	<table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Address</td> <td>9.3.106.58</td> <td> </td> </tr> </tbody> </table>	Type	Value	Actions	Address	9.3.106.58	 
Type	Value	Actions					
Address	9.3.106.58	 					
	 Add HMC						

Figura 67. Eseguire il rilevamento su ambiti specifici

- Per eseguire un rilevamento su un ambito specifico, fare clic sull'icona **Esegui**  per tale ambito.
- Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Esecuzione del rilevamento su ambiti dinamici VMWare

Procedura

- Nel pannello di navigazione, fare clic su **Ambiti di rilevamento > Ambiti dinamici VMWare**. Verrà visualizzata la pagina **Ambiti dinamici VMWare**.

Summary	<h1>VMware Dynamic Scopes</h1> <p>Users can define VMware Dynamic Scopes to collect detailed inventory from VMware vCenter Server and VMware ESXi. In addition to retrieving inventory information from the defined VMware vCenter Server or ESXi, TSA also queries managed virtual machines dynamically, without requiring users to create and maintain multiple scope definitions.</p>						
Activity Log							
Inventory Summary							
Discovery Scopes							
General Discovery Scopes							
Import General Scope Set							
HMC Dynamic Scopes							
VMware Dynamic Scopes							
Discovery Credentials							
Discovery Schedule							
Discovery History							
Discovery Settings							
	VMware Dynamic Scopes						
	<table border="1"> <thead> <tr> <th>Name</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>DyVM_Scope</td> <td>   </td> </tr> <tr> <td>dyVCenter_Scope</td> <td>   </td> </tr> </tbody> </table>	Name	Actions	DyVM_Scope	   	dyVCenter_Scope	   
Name	Actions						
DyVM_Scope	   						
dyVCenter_Scope	   						

Figura 68. Ambiti dinamici VMWare

- Fare clic sulla serie di ambiti che contiene l'ambito da rilevare. Verrà visualizzata la pagina **Serie di ambiti dinamici VMWare**. Questa pagina mostra tutti gli ambiti definiti per tale serie di ambiti.

Figura 69. Eseguire il rilevamento su ambiti dinamici VMWare

3. Per eseguire un rilevamento su un ambito specifico, fare clic sull'icona **Esegui**  per tale ambito.
4. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). Il rilevamento viene mostrato nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). Il rilevamento dovrebbe essere completato senza errori.

Cronologia rilevamento

È possibile visualizzare i dettagli di un rilevamento dopo il completamento e scaricare un file di log di diagnostica per il rilevamento.

Procedura

Per visualizzare la cronologia del rilevamento, attenersi a questa procedura:

1. Nel pannello di navigazione, fare clic su **Cronologia rilevamento**.
Verrà visualizzata la pagina **Cronologia rilevamento**. Viene visualizzato un elenco di voci di rilevamento. Ogni voce visualizza lo stato, il nome e l'ora di inizio e fine di un rilevamento.



Figura 70. Cronologia rilevamento

2. Per visualizzare maggiori informazioni su una voce nell'elenco **Voci di cronologia**, fare clic sul nome della voce di cronologia.
Il pannello **Informazioni voce** visualizza le informazioni sul rilevamento selezionato.
3. Per scaricare un file di log di diagnostica per un rilevamento, fare clic sull'icona **Scarica**  per il rilevamento.
4. Per eliminare un file di log di diagnostica per un rilevamento, fare clic sull'icona **Elimina**  per il rilevamento.

Pianificazione trasmissione

La trasmissione dei dati è pianificata per garantire che i dati rilevati siano inviati regolarmente al supporto IBM. È possibile visualizzare la pianificazione della trasmissione e i dettagli delle ultime trasmissioni, modificare la pianificazione della trasmissione e disabilitare le trasmissioni pianificate. È anche possibile inviare i dati a IBM in qualsiasi momento.

Visualizzazione della pianificazione della trasmissione

È possibile visualizzare le informazioni di riepilogo su una pianificazione di trasmissione.

Informazioni su questa attività

Per visualizzare la pianificazione della trasmissione, attenersi a questa procedura:

Procedura

Nel pannello di navigazione, fare clic su **Pianificazione trasmissione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Il pannello **Pianifica** visualizza la successiva esecuzione pianificata e l'ora. Il pannello **Cronologia** visualizza lo stato e ulteriori dettagli dei lavori di trasmissione correntemente in esecuzione e precedenti.

Modifica della pianificazione della trasmissione

TSA fornisce una pianificazione predefinita in base alla quale eseguire il processo di trasmissione a un determinato orario. È possibile modificare questa pianificazione in base alle esigenze.

Procedura

1. Nel pannello di navigazione, fare clic su **Pianificazione trasmissione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Il pannello **Pianifica** visualizza la successiva esecuzione pianificata e l'ora. Il pannello **Cronologia** visualizza lo stato e ulteriori dettagli dei lavori di trasmissione correntemente in esecuzione e precedenti.

2. Fare clic su **Modifica pianificazione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Figura 71. Modifica della pianificazione della trasmissione

- Utilizzare gli elenchi a discesa **A ore** e **A minuti** per selezionare il nuovo orario.
- Selezionare **Modalità di selezione giorno**.

Per giorno settimanale (dom-sab)

Per pianificare la trasmissione in giorni specifici di una settimana, selezionare l'opzione **Per giorno settimanale (dom-sab)**.

Figura 72. Per giorno settimanale (dom-sab)

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni della settimana.

Per data mensile (1-31)

Per pianificare la trasmissione in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni del mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

3. Fare clic su **Salva**.

Viene visualizzata di nuovo la pagina **Pianificazione trasmissione** con la nuova pianificazione.

Disabilitazione della pianificazione della trasmissione

È possibile disabilitare le trasmissioni di dati pianificate.

Procedura

Per disabilitare le trasmissioni pianificate, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Pianificazione trasmissione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

2. Fare clic su **Modifica pianificazione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

3. Nel pannello **Abilita pianificazione**, selezionare **Disabilita trasmissione pianificata**.

4. Fare clic su **Salva**.

Viene visualizzata la pagina **Pianificazione rilevamento** e il riquadro **Pianifica** mostra che il rilevamento pianificato è disabilitato. È possibile abilitare le trasmissioni pianificate facendo clic su **Abilita trasmissione pianificata**.

Esecuzione della trasmissione

È possibile eseguire una trasmissione su richiesta, invece che attendere la successiva trasmissione pianificata.

Procedura

1. Nel pannello di navigazione, fare clic su **Pianificazione trasmissione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Transmission Schedule ?

Previously collected data will be transmitted to IBM at the specified time.

Schedule

Next run: 12/13/19 9:35 AM GMT

Runs at: 09:35 AM on month day(s): 13, 14, 15

History

Status	Instance	State	Comments
✓	11/19/19 10:09 PM GMT	Complete	<ul style="list-style-type: none"> Last status: OK Last run: 11/19/19 10:09 PM GMT Last completed: 11/19/19 10:50 PM GMT Last duration: 40 mins,57 secs Initiator: admin
✓	11/19/19 9:13 PM GMT	Complete	<ul style="list-style-type: none"> Last status: OK Last run: 11/19/19 9:13 PM GMT Last completed: 11/19/19 9:44 PM GMT Last duration: 31 mins,12 secs Initiator: admin
✓	11/10/19 10:54 PM GMT	Complete	<ul style="list-style-type: none"> Last status: OK Last run: 11/10/19 10:54 PM GMT Last completed: 11/10/19 11:26 PM GMT Last duration: 32 mins,17 secs Initiator: admin

[Edit Schedule](#) [Run Transmission Now](#)

Figura 73. Esegui ora la trasmissione

2. Fare clic su **Esegui ora la trasmissione**.

Il pannello **Cronologia** viene aggiornato per indicare che la trasmissione è in esecuzione.

3. Esaminare la pagina **Riepilogo** (fare clic su **Riepilogo** nel pannello di navigazione). La trasmissione viene mostrata nel pannello **Riepilogo lavori**. La pagina **Riepilogo** viene aggiornata periodicamente per mostrare lo stato corrente di TSA. Una volta che il lavoro non è più elencato nel pannello **Riepilogo lavori**, esaminare il **Log attività** (fare clic su **Log attività** nel pannello di navigazione). La trasmissione dovrebbe essere completata senza errori.

Istantanea dei dati

È possibile generare e salvare una copia locale dei dati grezzi, non formattati che vengono raccolti da TSA senza trasmetterli a IBM. Inoltre, è possibile visualizzare gli ultimi dati trasmessi a IBM.

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Istantanea dei dati**. Verrà visualizzata la pagina **Istantanea dei dati**.



Figura 74. Istantanea dei dati

Nota: Il pulsante **Scarica ultima istantanea dei dati**, viene abilitato solamente quando è presente un'istantanea dei dati o una trasmissione completata.

2. Fare clic su **Genera istantanea dei dati ora** per raccogliere gli ultimi dati rilevati da TSA e generare una nuova istantanea dei dati. Verrà visualizzato il seguente messaggio - Istantanea dei dati in corso. Potrebbe richiedere fino a 2 ore. Visualizzare il log Attività o la pagina Riepilogo per conoscere lo stato. Fare clic su **Riepilogo** nel menu di navigazione per visualizzare la pagina **Riepilogo**. Il pannello **Riepilogo lavori** mostra lo stato della raccolta di istantanee dei dati fino al completamento. Fare clic su **Log attività** nel menu di navigazione per visualizzare lo stato di completamento della richiesta di istantanea dei dati.
3. Una volta completato il servizio di trasmissione o di istantanea dei dati, verrà visualizzata la **Data dell'istantanea dei dati**.



Figura 75. Data dell'istantanea dei dati

4. Fare clic su **Scarica ultima istantanea dei dati** per scaricare l'ultima istantanea dei dati. Specificare l'ubicazione del file risultante (*collection.tar.xz*). A seconda della quantità di dati, l'operazione può richiedere un certo tempo. Per estrarre il contenuto dell'archivio *.tar.xz*, utilizzare il programma di utilità *tar* (per Linux) o il programma di utilità *7-Zip* (disponibile per Linux e Windows).

Nota:

- Se è in corso un lavoro di raccolta o trasmissione, verrà visualizzato il seguente messaggio - Un lavoro di raccolta è attualmente in esecuzione. L'ultima istantanea dei dati è stata generata il <<timestamp>>. Scaricare questa raccolta?
 - Fare clic su **OK** per procedere con il download.
 - Fare clic su **Annulla** per annullare il download e attendere il completamento del lavoro di raccolta attualmente in esecuzione.

- Se non è in corso un lavoro di raccolta o trasmissione, verrà visualizzato il seguente messaggio - L'ultima istantanea dei dati è stata generata il <<timestamp>>. Scaricare questa raccolta?. Fare clic su **OK** per procedere con il download.

Visualizzazione del riepilogo dell'inventario

Utilizzare la pagina **Riepilogo inventario** per visualizzare il riepilogo degli elementi IT, come i sistemi di computer, i sistemi operativi e i sottosistemi di storage rilevati.

Fare clic su **Riepilogo inventario** nel pannello di navigazione per visualizzare la pagina **Riepilogo inventario**.

Inventory Summary ?

A general summary of IT elements that have been discovered. Some IT elements may not be represented on this summary. For a complete report with detailed information and analysis refer to the Technical Support Appliance reports from your IBM representative.

Inventory Summary	
Computer Systems (3)	<ul style="list-style-type: none"> HP-UX (1) AIX (1) Other Computer Systems (19)
Network Elements (0)	No elements discovered
Other Servers (0)	No elements discovered
Storage (0)	No elements discovered
Unknown IPs (0)	No elements discovered
Last generated: 6/7/17 2:47 PM BST	

[Download Inventory Summary](#)

Figura 76. Riepilogo inventario

La pagina Riepilogo inventario mostra sei differenti gruppi di elementi IT:

- **Hypervisor:** include gli hypervisor come HMC, IBM Flex System Manager, VMware, VIOS, ecc.
- **Computer:** include i sistemi di computer fisici.
- **Sistemi operativi:** include i sistemi operativi come AIX, Linux, ecc. in esecuzione in ambienti bare metal o virtualizzati.
- **Elementi di rete:** include gli switch e i router.
- **Storage:** include i sottosistemi di storage come i dispositivi di storage IBM XIV, IBM FlashSystem, EMC e HP. Inoltre, include anche i dispositivi a nastro.
- **IP sconosciuti:** i dispositivi che non possono essere classificati per motivi come i seguenti:
 - Il firewall blocca l'accesso al dispositivo.
 - Nessuna credenziale definita per il dispositivo. Visualizzare la pagina **Stato autenticazione** (**Strumenti** → **Stato autenticazione**) per informazioni sugli indirizzi IP e le credenziali associate.

– Non esistono sensori per questo tipo di dispositivo.

- La riga **Ultima generazione** indica l'ultima volta che è stato completato il lavoro di riepilogo dell'inventario.

Nota: I dati su questo pannello vengono visualizzati subito dopo l'avvio di TSA. Se si visualizza la pagina in questo intervallo, viene visualizzato un messaggio informativo: **Generazione del riepilogo inventario in corso**. Dopo che le informazioni sul riepilogo sono inizialmente inserite, sono aggiornate approssimativamente ogni 30 minuti. Per aggiornare manualmente, fare clic sull'icona **Aggiorna** del browser.

Ogni gruppo visualizza l'elenco di tipi di dispositivi e il conteggio per ogni tipo.

1. Fare clic su un qualsiasi hyperlink per il tipo di dispositivo per visualizzare la pagina **Dettagli riepilogo inventario**.

Elements		Element information
Name	Last Modified	
0000020062C2232C	6/16/15 2:33 AM BST	Context IP address: 198.51.100.0
192.0.2.0	6/16/15 3:19 AM BST	Manufacturer: IBM
1-2 of 2 results		Model: 9846-AE1
Results per page: 15 50 100		Serial number: 1331020

Figura 77. Dettagli riepilogo inventario

2. Selezionare un dispositivo nell'elenco per visualizzare le **Informazioni elemento** come *Indirizzo IP contesto, Produttore, Modello e Numero di serie*.

Nota: Per dispositivi rilevati da TSA, ma per i quali non sono state definite credenziali valide, non sono compilate le **Informazioni elemento**. TSA richiede un accesso corretto al dispositivo, al fine di fornire questi dettagli.

Fare clic su **Scarica riepilogo inventario** per scaricare un file contenente un riepilogo dei dispositivi rilevati.

Debug di problemi di rilevamento

Stato autenticazione

Utilizzare la pagina **Stato autenticazione** per visualizzare un riepilogo degli elementi IT, definiti nelle serie di ambiti e che presentano problemi di credenziali.

Per visualizzare lo stato di autenticazione, fare clic su **Strumenti** > **Stato autenticazione** nel pannello di navigazione. Viene visualizzata la pagina **Stato autenticazione**.

- Summary
- Activity Log
- Inventory Summary
- Discovery Scopes
- Discovery Credentials
- Discovery Schedule
- Discovery History
- Discovery Settings
- Transmission Schedule
- Administration
- Tools
 - Network Tools
 - Unknown Devices
 - Authentication Status
 - DB Tools
 - Setup Wizard
 - Documentation

Authentication Status ?

This page provides a summary of the IT elements, defined in scope sets, that have been identified to potentially have issues with credentials. Either no credentials are defined for the associated scope set, credentials are defined for the scope set but none are successful, or a credential that was successful in the past was not successful on the latest discovery attempt. This information should help to determine where new credentials should be created, or where existing credentials should be updated with the correct password.

Note:
Once the problem preventing an element from being identified is resolved, it will no longer display on this list.

IP Address		
Address	Last Attempted	Last Successful
9.155.120.226	2/12/20 6:28:14 AM GMT	
9.182.192.107	3/10/20 4:14:43 AM GMT	
9.5.12.187	2/26/20 4:12:57 AM GMT	
9.5.12.201	2/26/20 4:12:57 AM GMT	
9.5.54.240	2/26/20 4:12:57 AM GMT	
9.5.95.56	2/26/20 4:12:57 AM GMT	

1 - 6 of 6 entries Entries per page: 20 | 50 | 100

Device information

Address:
9.155.120.226

Last Attempted:
2/12/20 6:28:14 AM GMT

Last Successful:
2/12/20 6:28:14 AM GMT

Ports open:
[22, 23, 80, 427, 443, 445, 1750, 1751, 2463, 5986, 5988, 5989, 7778]

Last successful credential used:
TS7760_Cred

Credentials associated with scope:
TS7760_Cred

Scopes including this IP address:
TS7760_Scope

Figura 78. Stato autenticazione

Lo stato visualizza tutti gli IP dispositivo per cui sono stati notificati problemi di credenziali. Di seguito sono indicati i motivi per cui si potrebbero verificare problemi:

- Credenziali non definite per la serie di ambiti associata.
- Sono definite credenziali per la serie di ambiti ma non sono corrette.
- Le credenziali erano corrette in passato ma non lo sono per l'ultimo tentativo di rilevamento.

Fare clic sul rispettivo link di indirizzo IP per visualizzare informazioni sul dispositivo come *Ultimo tentativo*, *Ultimo tentativo riuscito*, *Porte aperte*, *Ultima credenziale utilizzata correttamente*, *Data dell'ultima modifica della credenziale*, *Credenziale associata all'ambito* e *Ambiti che includono questo indirizzo IP*. Queste informazioni sono utili per determinare dove devono essere create nuove credenziali o dove le credenziali esistenti devono essere aggiornate con la password corretta.

Nota: Una volta risolto il problema di credenziale per un dispositivo, il relativo IP dispositivo non viene più visualizzato nell'elenco.

Dispositivi sconosciuti

È possibile visualizzare le informazioni sui dispositivi che TSA ha rilevato, ma non è in grado di identificare completamente.

Per visualizzare questi dispositivi sconosciuti, fare clic su **Strumenti > Dispositivi sconosciuti** nel pannello di navigazione. Viene visualizzata la pagina **Dispositivi sconosciuti**.

È possibile fare clic su qualsiasi voce nell'elenco di IP sconosciuti per visualizzare ulteriori informazioni su tale dispositivo.

Capitolo 6. Configurazione di attività amministrative

Informazioni sullo stato

TSA fornisce informazioni di riepilogo, log e report per permettere di trovare rapidamente informazioni sui lavori, gli inventari rilevati e informazioni sul prodotto.

È possibile visualizzare un livello alto di informazioni di riepilogo su lavori, inventario e informazioni sul prodotto facendo clic su **Riepilogo** nel pannello di navigazione. La pagina **Riepilogo** si aggiorna frequentemente per visualizzare le informazioni di riepilogo più recenti. La pagina **Riepilogo** include le seguenti informazioni:

- **Stato sistema**

Il pannello **Stato sistema** visualizza lo stato dei servizi correnti e le attività in esecuzione. È possibile visualizzare le pagine per i servizi visualizzati facendo clic sul nome del servizio nel pannello **Stato sistema**.

- **Riepilogo lavori**

Il pannello **Riepilogo lavori** mostra un riepilogo dei lavori correnti.

- **Riepilogo inventario**

Il pannello **Riepilogo inventario** mostra un elenco degli inventari rilevati.

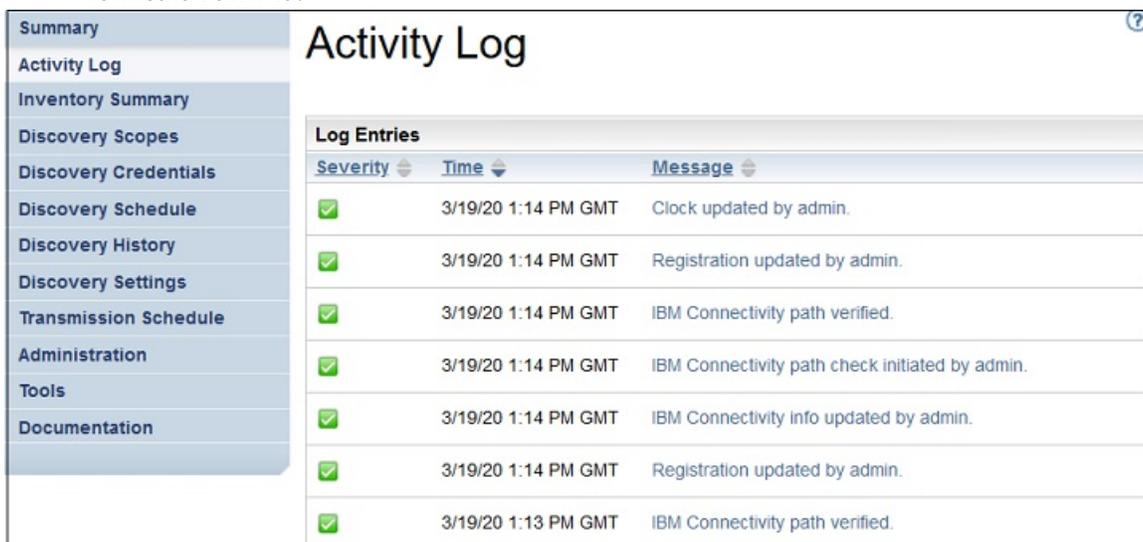
- **Informazioni sul prodotto**

Il pannello **Informazioni sul prodotto** mostra il nome host e l'ID di TSA.

Visualizzazione del log attività

Il log attività visualizza i messaggi di log per i processi di rilevamento e trasmissione. È possibile fare clic sulle voci nel log attività per visualizzare maggiori informazioni.

È possibile visualizzare il log attività facendo clic su **Log attività** nel pannello di navigazione. Viene visualizzato un elenco di voci di log. Ogni voce visualizza il messaggio, la severità e l'ora in cui si è verificata l'attività.



Activity Log		
Log Entries		
Severity	Time	Message
✓	3/19/20 1:14 PM GMT	Clock updated by admin.
✓	3/19/20 1:14 PM GMT	Registration updated by admin.
✓	3/19/20 1:14 PM GMT	IBM Connectivity path verified.
✓	3/19/20 1:14 PM GMT	IBM Connectivity path check initiated by admin.
✓	3/19/20 1:14 PM GMT	IBM Connectivity info updated by admin.
✓	3/19/20 1:14 PM GMT	Registration updated by admin.
✓	3/19/20 1:13 PM GMT	IBM Connectivity path verified.

Figura 79. Log attività

Nota: Poiché i rilevamenti sono eseguiti su singole serie di ambiti, potrebbero esserci più voci di log per un rilevamento completo.

Per visualizzare dettagli estesi su una voce del log attività, fare clic sul messaggio per tale voce.

Per salvare i file di log sul computer, fare clic su **Scarica tutti i log**.

Per cancellare il log, fare clic su **Cancella log**.

Visualizzazione dell'archivio ripulitura inventario

È possibile visualizzare l'inventario che viene ripulito in base al periodo dormiente specificato in **Pianificazione pulitura inventario**

Informazioni su questa attività

Per visualizzare l'inventario eliminato, attenersi a questa procedura:

Procedura

1. Sulla pagina **Pianificazione pulitura inventario**, fare clic su **Mostra archivio pulitura**. Viene visualizzata la pagina **Archivio ripulitura inventario**.

Inventory Cleanup Archive

This page allows you to view and download a list of inventory elements that have not been detected by the discovery job for a time longer than the defined dormant age and have been purged from inventory. These elements will be archived for one year after the date they were purged.

Archived Inventory Entries	
Display Name: c642a-m2b10.pok.stglabs.ibm.com	Last Seen: 2015-10-10 09:38 CDT
Name: c642a-m2b10	Cleaned Up: 2015-11-11 11:19 CST
Subtype: LinuxUnitaryComputerSystem	Manufacturer: IBM
Scope: ?	Model: 8853AC1
Context IP: 9.57.20.84	Serial Number: KQHYLFC
Display Name: c642a-m2b9.pok.stglabs.ibm.com	Last Seen: 2015-10-10 09:38 CDT
Name: c642a-m2b9	Cleaned Up: 2015-11-11 11:19 CST
Subtype: LinuxUnitaryComputerSystem	Manufacturer: IBM
Scope: ?	Model: 7870AC1
Context IP: 9.57.20.83	Serial Number: KQXXDTH

[Back to top](#)

Options

Order by: Cleaned Up

Reverse order

Compact view

Download

Figura 80. Archivio pulitura inventario

2. Sulla pagina **Archivio ripulitura inventario**, è possibile visualizzare gli elementi cancellati dall'inventario come parte del processo di pulitura.

Nota:

- È possibile visualizzare le informazioni sull'inventario in questo archivio solo per un anno. Dopo un anno, le informazioni sull'archivio vengono cancellate.
- L'archivio sarà vuoto (cioè nessun oggetto è cancellato), se tutte le destinazioni definite sono state attivamente rilevate nell'ultimo anno.

3. Utilizzare il pannello **Opzioni** per riordinare i dettagli dell'inventario.

- a) Selezionare la proprietà **Ordina per** nel pannello **Opzioni** e fare clic su **Applica** per ordinare la vista dei dettagli di inventario.
- b) Selezionare l'opzione **Inverti ordine** per visualizzare i dettagli nell'ordine inverso della proprietà selezionata.
- c) Selezionare l'opzione **Vista compatta** per visualizzare un riepilogo dell'inventario.

4. Fare clic su **Come file di testo** o **Come file CSV** per scaricare i dettagli dell'inventario. Salvare i dettagli dell'inventario per gestire i dati localmente e preservare i dati sul computer per un periodo più lungo (più di un anno). I dati preservati in questo archivio sono conservati solo per un anno e poi cancellati.

Password

Utilizzare le password per proteggere gli account utente TSA.

Modifica della password

Modificare la password utente di TSA.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Password**.

Viene visualizzata la pagina **Password**.

2. Immettere la password corrente nel campo **Password corrente**.
3. Immettere la nuova password nel campo **Nuova password**.

La password deve rispettare le seguenti regole:

- Deve essere lunga almeno 8 caratteri
- Deve contenere almeno un carattere alfabetico e un carattere non alfabetico
- Non deve contenere il nome utente
- Non deve essere uguale a una delle precedenti otto password
- Deve essere modificata almeno una volta ogni 90 giorni, ma non deve essere modificata più di una volta al giorno

4. Immettere nuovamente la nuova password nel campo **Conferma password**.

Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.

5. Fare clic su **Salva**.

Operazioni successive

Importante: Non è possibile ripristinare una password, pertanto se la si perde o dimentica, non è possibile accedere a TSA per modificare le credenziali. Se si perde o si dimentica la password per un account utente o account amministratore (se si dispone di più account), contattare l'amministratore TSA. Se si perde o si dimentica la password per l'account amministratore predefinito (inviato con l'appliance), contattare il supporto IBM. Per maggiori informazioni, consultare la sezione [“Accesso a Technical Support Appliance” a pagina 23](#).

Sicurezza

È possibile accedere e modificare le funzioni di sicurezza e i programmi di utilità per TSA.

La pagina **Sicurezza** elenca i programma di utilità di sicurezza disponibili. Su questa pagina, è possibile modificare le impostazioni di timeout della sessione o modificare la durata massima della password per tutti gli account utente.

Modifica delle impostazioni di timeout sessione

Per motivi di sicurezza, l'utente viene disconnesso da TSA dopo un certo periodo di inattività. È possibile impedire a TSA di effettuare la disconnessione automatica o modificare l'intervallo di tempo prima della disconnessione.

Disabilitazione del timeout di sessione

È possibile impedire a TSA di effettuare la disconnessione automatica dell'utente dopo un periodo di inattività disabilitando il timeout della sessione.

Procedura

1. Selezionare la casella di spunta **Disabilita timeout di sessione**.
2. Fare clic su **Modifica impostazioni di timeout sessione**.

Modifica del valore di timeout della sessione

Per impostazione predefinita, l'utente viene scollegato dopo 20 minuti di inattività. È possibile aumentare questo intervallo di tempo modificando il valore di timeout della sessione.

Procedura

1. Deselezionare la casella di spunta **Disabilita timeout di sessione**.
2. Nel campo **Timeout sessione**, immettere il tempo, in secondi, che deve trascorrere prima che TSA disconnetta l'utente.

Nota: Il valore di timeout per questa sessione non può essere inferiore a 20 minuti.

3. Fare clic su **Modifica impostazioni di timeout sessione**.

Modifica della durata della password

Come misura di sicurezza, ogni utente è forzato a modificare la password di accesso a TSA dopo un numero di giorni specificato. Per impostazione predefinita, la durata massima di una password è di 90 giorni, ma è possibile modificare tale durata in 30 o 60 giorni.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Sicurezza**. Verrà visualizzata la pagina **Sicurezza**.
2. Nella pagina **Sicurezza**, scorrere verso il basso per visualizzare il pannello **Durata massima password**.
3. Nel pannello **Durata massima password**, selezionare la durata (30 giorni, 60 giorni o 90 giorni) dall'elenco a discesa **Durata massima**.
4. Fare clic su **Modifica durata massima password** per aggiornare. Viene visualizzato il messaggio di conferma *Durata massima password aggiornata*.

Backup e ripristino

È possibile eseguire il backup e il ripristino della configurazione di TSA.

Importante: Si consiglia caldamente di eseguire un backup con regolarità. Inoltre, si dovrebbe eseguire un backup dopo che sono state apportate modifiche alle serie di ambiti o alle credenziali.

Data del backup

Indica la data e l'ora in cui è stato effettuato il backup più recente.

Riepilogo configurazione

Utilizzare questa opzione per visualizzare un riepilogo della configurazione corrente di TSA prima di salvarla.

Per visualizzare il riepilogo della configurazione di TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione > Backup e ripristino**. Viene visualizzata la pagina **Backup e ripristino**.

2. Fare clic su **Visualizza riepilogo** per visualizzare il riepilogo della configurazione corrente di TSA. Le informazioni visualizzate mostrano la configurazione che TSA salva se viene eseguito un backup.

Nota: Queste informazioni sono visualizzate in una finestra a comparsa. Se il browser web blocca i pop-up, occorre consentirgli di visualizzare i pop-up da TSA.

Nella pagina **Riepilogo**, la sezione **Backup** visualizza le informazioni correlate allo stato del backup con i seguenti messaggi:

- Una icona *OK* (✓), se l'ultimo backup effettuato è entro 60 giorni.
- Una icona *Avvertenza* (⚠), se il backup non è stato effettuato per più di 60 giorni e meno di o entro 90 giorni.
- Una icona *Errore* (✗), se il backup non è stato effettuato per più di 90 giorni.

Backup

Utilizzare questa opzione per salvare una copia della configurazione di TSA.

Per eseguire il backup della configurazione di TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Backup e ripristino**. Viene visualizzata la pagina **Backup e ripristino**.

The screenshot shows the 'Backup and Restore' page in a web application. On the left is a navigation sidebar with categories: Summary, Activity Log, Inventory Summary, Discovery Scopes, Discovery Credentials, Discovery Schedule, Discovery History, Discovery Settings, Transmission Schedule, Administration (with sub-items: Registration, License, Clock, Network, IBM Connectivity, User Accounts, Password, Security, Certificates, Backup and Restore, Update, Logging and Trace, Scheduled Maintenance, Data Snapshot, Shutdown), Tools, and Documentation. The 'Backup and Restore' item is highlighted with a red box. The main content area has a title 'Backup and Restore' and a help icon. Below the title is a description: 'This page allows you to backup and restore the system configuration.' and a note: 'Asterisks (*) indicate mandatory fields that are required to complete this action.' There are three main sections: 1. 'Backup Date' with a message 'Backup has not been performed.' 2. 'Configuration Summary' with a description 'Use this action to view the current configuration summary before backing it up.' and a 'View Summary' button. 3. 'Backup' with a description 'Use this action to download a copy of the current configuration to the system on which this Web interface is running. You must enter a password to protect the configuration file.' It includes 'Password: *' and 'Confirm Password: *' fields, a 'Specify a password to protect the configuration file.' instruction, and a 'Backup' button. 4. 'Restore' with a description 'Use this action to restore a saved configuration from file.' and instructions 'Select configuration file to restore, then click 'Restore'. You must enter a password if the configuration file is protected with a password.' It includes a 'File: *' field with a 'Choose File' button and 'No file chosen' text, a 'Password:' field, a 'Specify the password that was used to protect the configuration file.' instruction, and a 'Restore' button.

Figura 81. Backup e ripristino

2. Immettere una password nel pannello **Backup** per proteggere il file di configurazione.

3. Immettere nuovamente la password nel campo **Conferma password**. Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.

Nota: È necessario conservare la password in modo sicuro poiché sarà necessaria durante il ripristino.

4. Fare clic su **Backup** e salvare il file compresso di configurazione di backup sul sistema.

Nota: Il file di configurazione di backup generato può essere aperto solo in TSA.

Nota: Se la password admin è stata modificata di recente, effettuare un backup dopo la modifica della password e utilizzare l'ultimo file di backup per il ripristino.

Ripristino

Utilizzare questa opzione per ripristinare una copia della configurazione precedentemente salvata.

Per ripristinare la configurazione di TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione > Backup e ripristino**. Viene visualizzata la pagina **Backup e ripristino**.
2. Fare clic su **Scegli file** per individuare e selezionare il file di configurazione che si desidera ripristinare.
3. Immettere la password utilizzata per eseguire il backup del file di configurazione.
4. Fare clic su **Ripristina**.

Il lavoro di ripristino viene visualizzato nel pannello Riepilogo lavori della pagina **Riepilogo**. Una volta completato il ripristino, viene richiesto di riavviare il sistema.

Nota: Il ripristino da un backup elimina le configurazioni correnti. Tutte le configurazioni, incluso definizioni di ambito e credenziali, vengono sostituite con quelle del backup.

Nota: Assicurarsi che lo stato di Discovery Manager sia OK (✓) nella pagina **Riepilogo** quando si eseguono le operazioni di backup e ripristino. Se Discovery Manager non è in esecuzione, si riceve il messaggio - "Discovery Manager non in esecuzione. Assicurarsi che lo stato di Discovery Manager sia contrassegnato con un segno di spunta verde nel pannello Riepilogo prima di riprendere l'attività (generalmente massimo 10 minuti)." Se Discovery Manager non è in esecuzione dopo 10 minuti, contattare il supporto IBM.

Aggiornamento

È possibile controllare la disponibilità di aggiornamenti per TSA e scaricarli.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Aggiorna**. Viene visualizzata la pagina **Aggiornamento**.

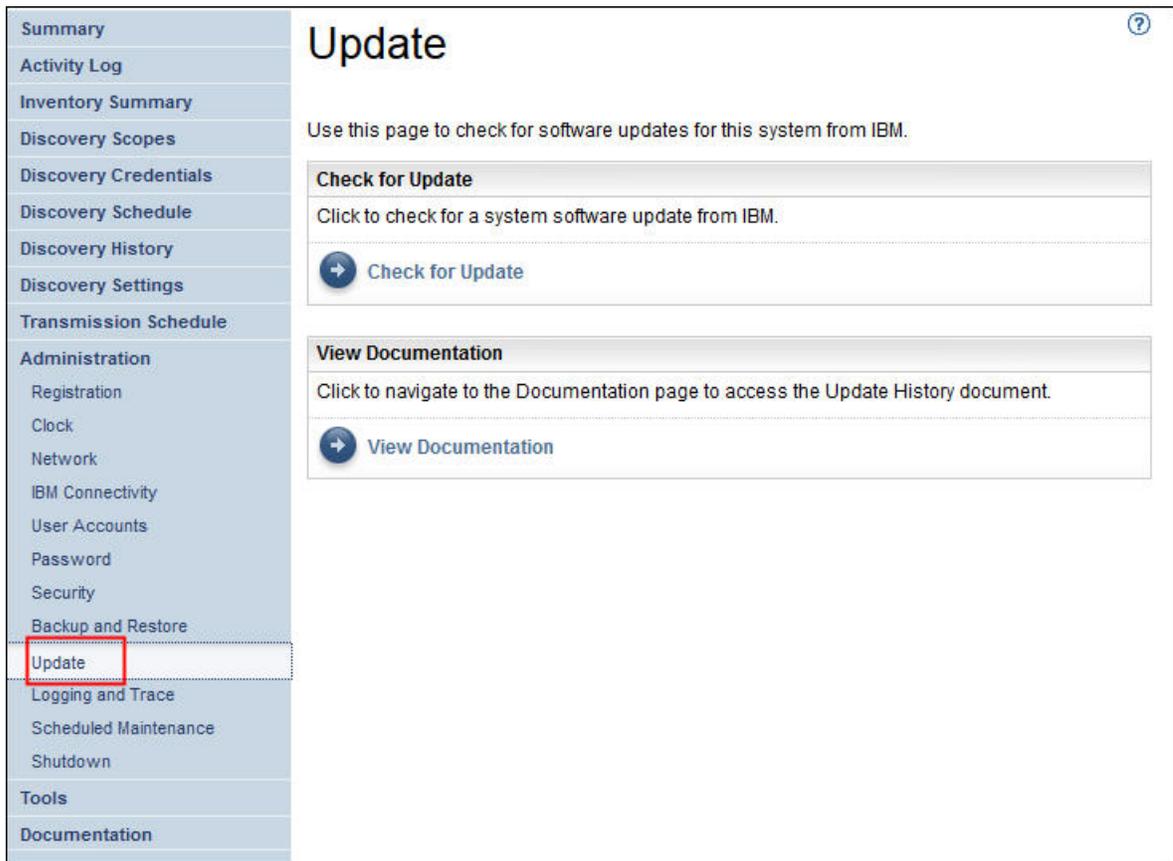


Figura 82. Aggiornamento

2. Fare clic su **Controlla aggiornamenti**.

La pagina **Disponibilità degli aggiornamenti** elenca gli eventuali aggiornamenti disponibili.

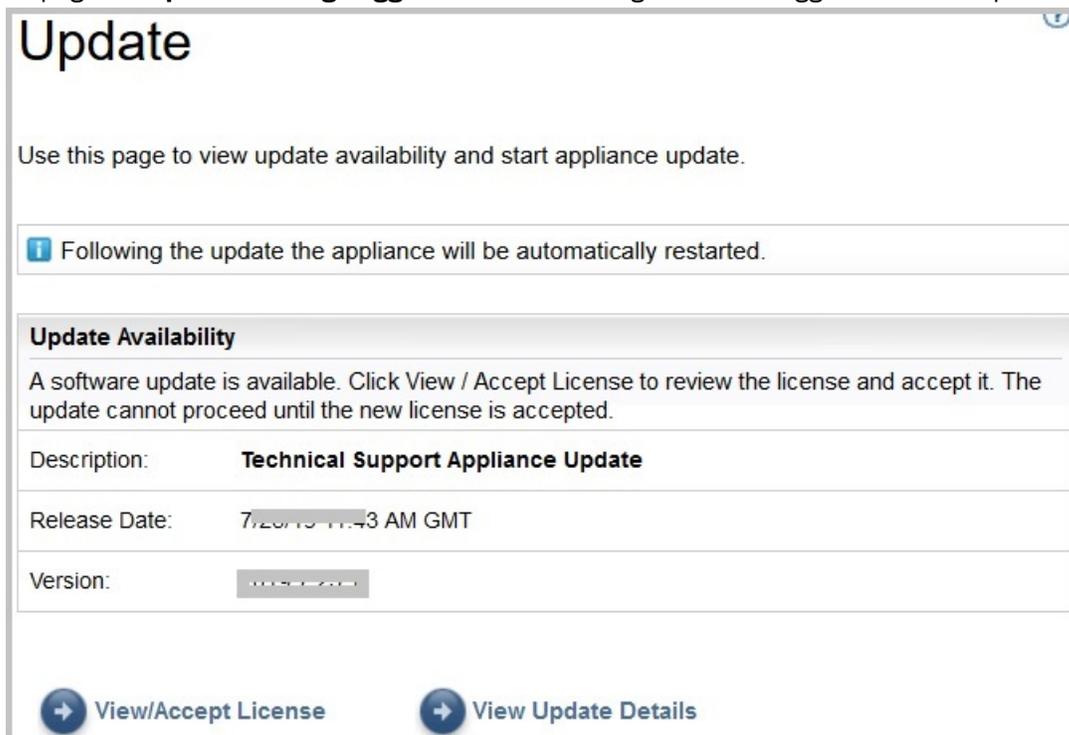


Figura 83. Disponibilità degli aggiornamenti

- a) Per alcune nuove release di TSA, è necessario accettare un nuovo accordo di licenza prima di procedere con l'aggiornamento. Se esiste una nuova licenza, fare clic su **Visualizza/Accetta licenza**; verrà visualizzata la pagina **Accordo di licenza**.
- b) Fare clic sul pulsante **Accetta** sulla pagina **Accordo di licenza** per accettare il nuovo accordo di licenza. Viene visualizzata nuovamente la pagina **Aggiornamento** con il pulsante **Esegui ora l'aggiornamento**. Se non è richiesto di accettare un nuovo accordo di licenza, non viene visualizzato il pulsante **Visualizza/Accetta licenza** ed è possibile procedere facendo clic sul pulsante **Esegui ora l'aggiornamento**.

Nota:

- Una volta accettata la licenza, non viene più visualizzato il pulsante **Visualizza/Accetta licenza**.
 - Nel pannello di navigazione, fare clic su **Amministrazione** > **Licenza** per visualizzare l'Accordo di licenza più recente accettato.
- c) Per installare gli aggiornamenti, fare clic su **Esegui ora l'aggiornamento**.

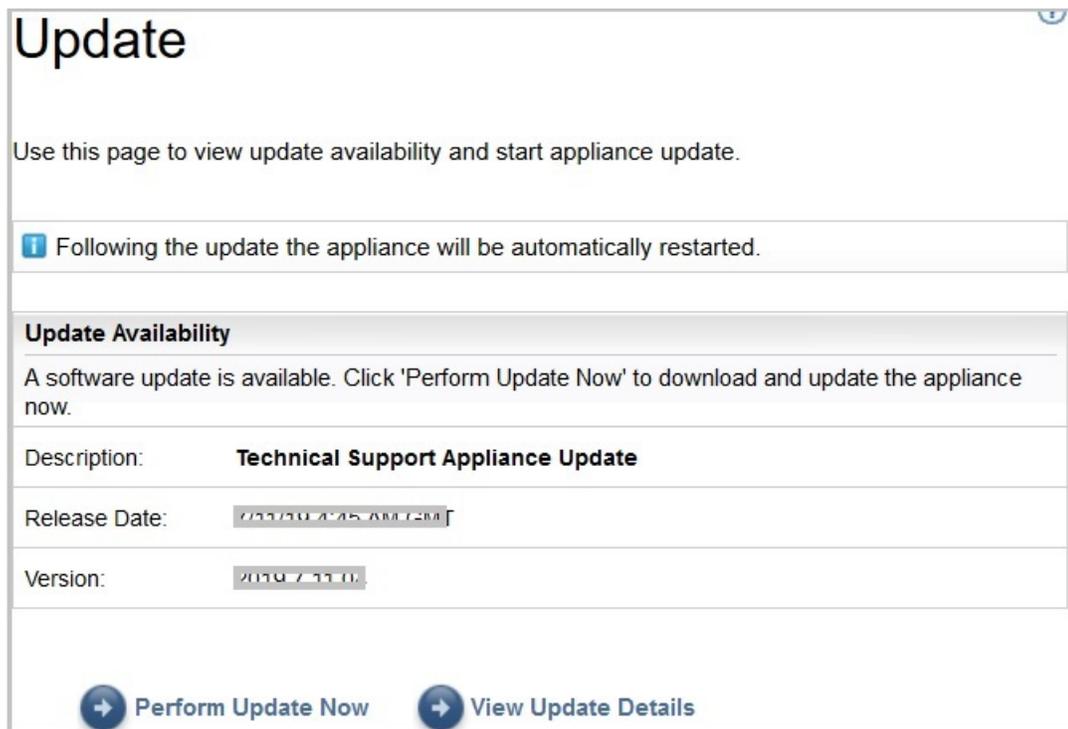


Figura 84. Esegui ora l'aggiornamento

Una volta completato l'aggiornamento, TSA viene riavviato automaticamente.

- d) Per visualizzare le informazioni relative ai contenuti dell'aggiornamento, fare clic su **Visualizza dettagli dell'aggiornamento**.

Abilitazione della manutenzione pianificata

Perché TSA funzioni in maniera ottimale, si consiglia di abilitare la funzione di manutenzione pianificata.

Informazioni su questa attività

Il lavoro di manutenzione pianificata garantisce prestazioni ottimali di TSA. È possibile sempre abilitare o disabilitare questa funzione. Se si abilita la manutenzione pianificata, è possibile impostare l'ora e il giorno per l'esecuzione automatica della manutenzione. Viene visualizzato lo stato della manutenzione pianificata nella sezione **Stato del sistema** della pagina **Riepilogo**.

Se si pianifica il lavoro di manutenzione, il sistema si riavvia automaticamente dopo la manutenzione e all'utente verrà notificato il riavvio del sistema un'ora prima che si verifichi. Ad esempio, A causa di manutenzione pianificata, un lavoro di riavvio del sistema verrà accodato tra 59 minuti.

Importante: Non pianificare la manutenzione dell'appliance entro 30 minuti da altri lavori pianificati, come il rilevamento della trasmissione o la ripulitura dell'inventario. Se la manutenzione è pianificata entro 30 minuti da altri lavori pianificati, il TSA non può eseguire tali lavori.

Procedura

Per modificare la pianificazione della manutenzione, completare le seguenti operazioni:

1. Nel pannello di navigazione, fare clic su **Manutenzione pianificata**.

La pagina **Manutenzione pianificata** visualizza la **pianificazione** per la successiva esecuzione pianificata e l'ora. La sezione **Cronologia** visualizza lo stato e ulteriori dettagli dei lavori di manutenzione correntemente in esecuzione e precedenti.

2. Sulla pagina **Manutenzione pianificata**, fare clic su **Modifica pianificazione**.

- a) Nel pannello **Abilita pianificazione**, selezionare se si desidera abilitare o disabilitare la manutenzione pianificata.
- b) Se si sceglie di abilitare l'attività di manutenzione pianificata, selezionare gli elenchi **A ore** e **A minuti** per selezionare il nuovo orario.
- c) Selezionare **Modalità di selezione giorno**. Per pianificare la manutenzione in giorni specifici di una settimana, selezionare l'opzione **Settimanalmente per giorni (Dom - Sab)** o per pianificare la manutenzione in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.
- d) Selezionare la casella di spunta appropriata per il campo **Nei giorni** per selezionare altri o differenti giorni della settimana o mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

3. Fare clic su **Salva**.

Viene visualizzata di nuovo la pagina **Manutenzione pianificata** con la nuova pianificazione.

Registrazione e traccia

È possibile visualizzare e modificare le impostazioni di traccia della diagnostica di TSA. È anche possibile modificare le impostazioni per i livelli di traccia del Discovery Manager. La modifica di tali informazioni può influenzare le prestazioni, per cui effettuarla solo se indicato dal supporto IBM.

1. Nel pannello di navigazione, fare clic su **Amministrazione > Registrazione e traccia**. Viene visualizzata la pagina **Registrazione e traccia**. Il pannello **Livello di traccia TSA** presenta l'impostazione di traccia corrente (Errore, Avvertenza, Informazione, Debug o Traccia).

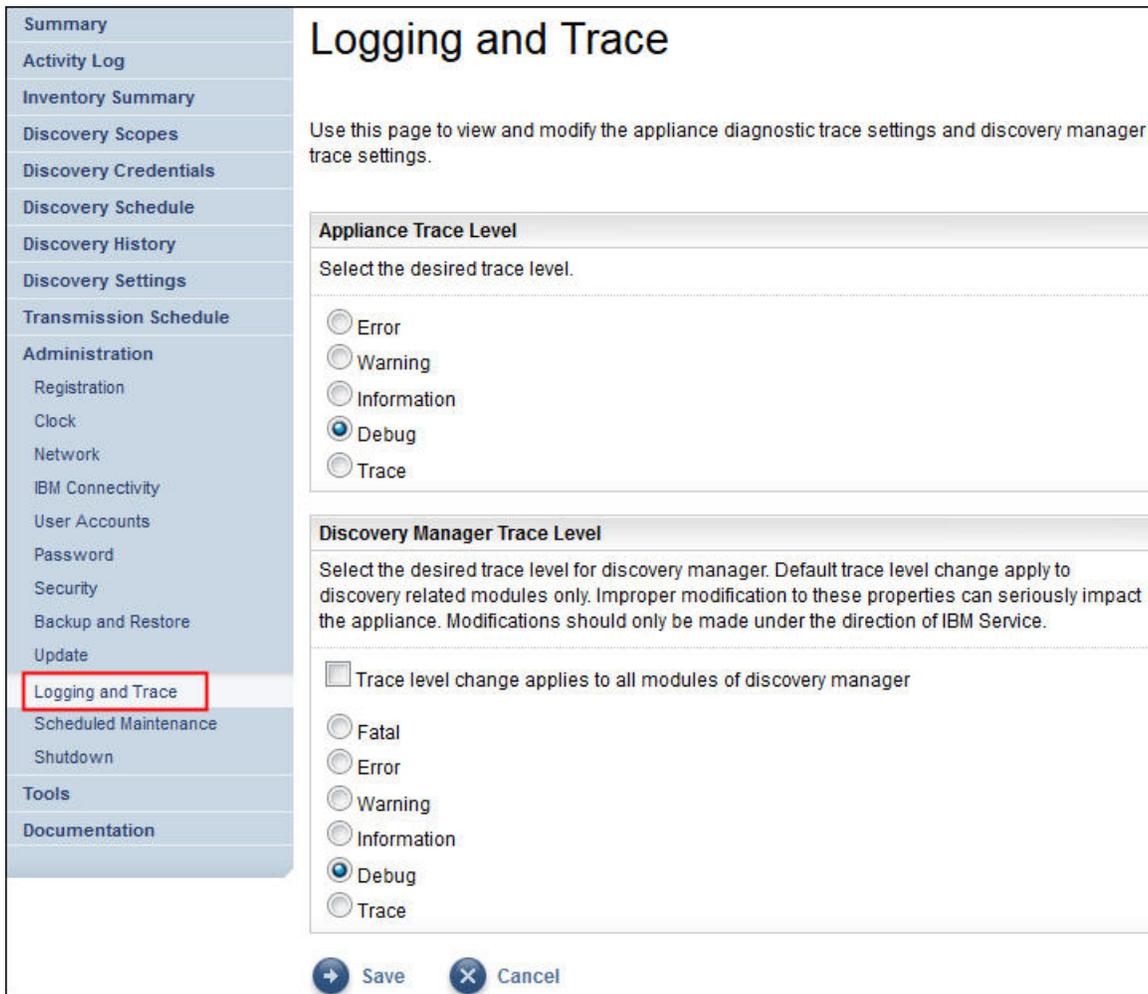


Figura 85. Registrazione e traccia

2. Se necessario, è possibile modificare l'impostazione di traccia nel pannello **Livello di traccia TSA**, facendo clic sul pulsante di scelta accanto all'impostazione di traccia desiderata.
3. Fare clic su **Salva**.

Nota: Per impostazione predefinita, il livello di traccia per i pannelli *Livello di traccia TSA* & *Livello di traccia Discovery Manager* è impostato su **Debug**.

Per visualizzare e modificare le impostazioni di **Livello di traccia Discovery Manager**, attenersi alla seguente procedura:

Importante: Effettuare modifiche a questa sezione solo se indicato da IBM Service.

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Registrazione e traccia**. Viene visualizzata la pagina **Registrazione e traccia** che indica l'impostazione di traccia corrente.
2. Selezionare **La modifica dei livelli di traccia si applica a tutti i moduli di Discovery Manager** se si desidera che il livello di traccia sia applicato a tutti i moduli di Discovery Manager.
3. Selezionare il pulsante di scelta accanto all'impostazione di traccia desiderata.
4. Fare clic su **Salva**.

Arresta

È possibile sospendere o riprendere le operazioni TSA o arrestare e poi riavviare o spegnere il TSA.

Il completamento dell'arresto richiede diversi minuti.

Summary

Activity Log

Inventory Summary

Discovery Scopes

Discovery Credentials

Discovery Schedule

Discovery History

Discovery Settings

Transmission Schedule

Administration

Registration

Clock

Network

IBM Connectivity

User Accounts

Password

Security

Backup and Restore

Update

Logging and Trace

Scheduled Maintenance

Shutdown

Tools

Documentation

Shutdown

This page provides options for powering off, restarting, suspending or resuming the system.

Suspend Operations

This action will temporarily stop the system until manually resumed. Scheduled discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted or manually invoked. Click "Suspend" if you want to continue and suspend the system.

➔ Suspend

Resume Operations

This action will resume suspended discovery and transmission operations. Your infrastructure collected data will again be reported on by the system. Click "Resume" if you want to continue and resume the system.

➔ Resume

Shutdown and Restart

This action will shutdown followed by a restart of the system. All existing network connections will be temporarily lost as a result. You will need to open a new browser and re-login to get back in to the user interface. Click "Restart" if you want to continue and restart the system.

➔ Restart

Shutdown and Power Off

This action will shutdown and power off the system. All discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted. Click "Shutdown" if you want to continue and stop the system.

➔ Shutdown

Figura 86. Arresta

Sospendi operazioni

Questa azione arresta temporaneamente TSA. Tutte le operazioni di rilevamento e trasmissione vengono arrestate e nessuna informazione viene riportata a IBM finché non vengono riprese le operazioni.

Per sospendere le operazioni TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Arresta**. Viene visualizzata la pagina **Arresta**.
2. Fare clic su **Sospendi**.

Riprendi operazioni

Questa azione riprende il TSA temporaneamente arrestato. Tutte le operazioni di rilevamento e trasmissione vengono riprese e le informazioni vengono riportate a IBM come pianificato.

Per riprendere le operazioni TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Arresta**. Viene visualizzata la pagina **Arresta**.
2. Fare clic su **Riprendi**.

Arresta e riavvia

Questa azione arresta e riavvia TSA. Tutte le connessioni di rete esistenti vengono temporaneamente perse. È necessario aprire un nuovo browser e riaccedere.

Per arrestare e riavviare TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Arresta**. Viene visualizzata la pagina **Arresta**.
2. Fare clic su **Riavvia**.

Arresta e spegni

Questa azione arresta e spegne TSA. Tutte le operazioni di rilevamento e trasmissione cesseranno e l'infrastruttura non verrà riattivata finché non si riavvia il TSA.

Per arrestare e spegnere TSA, attenersi alla seguente procedura:

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Arresta**. Viene visualizzata la pagina **Arresta**.
2. Fare clic su **Arresta**.

Nota: Dopo l'arresto dell'appliance, è necessario accendere il TSA utilizzando l'interfaccia Web VMware ESXi o Hyper-V Manager.

Strumenti

TSA fornisce strumenti per aiutare durante la configurazione dell'ambiente TSA.

È possibile accedere a questi strumenti facendo clic su **Strumenti** nel pannello di navigazione.

Strumenti di rete

Utilizzare la pagina **Strumenti di rete** per ottenere informazioni e strumenti di diagnostica per i protocolli di rete utilizzati da TSA.

Per accedere a questi strumenti di diagnostica, fare clic su **Strumenti** > **Strumenti di rete** nel pannello di navigazione. Viene visualizzata la pagina **Strumenti di rete**.

Viene visualizzata la pagina Strumenti di rete suddivisa in schede. Fare clic su una scheda per visualizzare la pagina corrispondente a tale scheda.

Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Network Tools
Unknown Devices
Authentication Status
DB Tools
Documentation

Network Tools

This page allows you to obtain network diagnostic information about the appliance's network protocols.

Ping Traceroute Test SSH Interfaces Ethernet Address Routes ARP Sockets IPs

Enter the TCP/IP Address or Hostname to ping.

IP address/hostname: * 10.10.10.10

➔ Ping

Figura 87. Strumenti di rete

Ping

Utilizzare questa pagina per inviare una richiesta echo a un host remoto per controllare se l'host è accessibile e ricevere informazioni sul nome host o l'indirizzo IP.

Tracciamento della route

Utilizzare questa pagina per visualizzare il percorso dei pacchetti a un host remoto.

Verifica SSH

Utilizzare questa pagina per verificare se un host remoto è accessibile con SSH utilizzando le credenziali di rilevamento definite per l'host.

Interfacce

Utilizzare questa pagina per visualizzare le statistiche per le interfacce di rete attualmente configurate.

Ethernet

Utilizzare questa pagina per visualizzare le impostazioni per le schede Ethernet attualmente configurate.

Indirizzo

Utilizzare questa pagina per visualizzare gli indirizzi IP per le interfacce di rete attualmente configurate.

Route

Utilizzare questa pagina per visualizzare le tabelle di instradamento IP kernel e le interfacce di rete corrispondenti.

ARP

Utilizzare questa pagina per visualizzare il contenuto delle connessioni ARP (Address Resolution Protocol).

Socket

Utilizzare questa pagina per visualizzare le informazioni sui socket TCP/IP.

IP

Utilizzare questa pagina per visualizzare le informazioni sulle regole di filtro dei pacchetti IP.

Nota: Il nome host immesso non deve contenere caratteri di sottolineatura ("_").

Strumenti database

Utilizzare la pagina **Strumenti database** per eseguire le operazioni di manutenzione dei dati. Si consiglia di utilizzare queste funzioni solo quando indicato dal supporto IBM.

È possibile eseguire le seguenti operazioni sul database:

Ricreazione del database inventario

Quando si ricrea il database inventario, tutti i dati dell'inventario vengono persi. Inoltre, le credenziali vengono perse se la casella di spunta **Preserva credenziali** è deselezionata o Discovery Manager non è disponibile.

Per ricreare il database, completare le seguenti operazioni:

1. Nel pannello di navigazione, fare clic su **Strumenti > Strumenti DB**.
2. Selezionare la casella di spunta **Preserva credenziali** nella sezione **Ricrea database inventario** per conservare tutte le credenziali di rilevamento. Se non si seleziona, le credenziali vengono perse e sarà necessario configurare di nuovo tutte le credenziali. Per ulteriori informazioni sulle credenziali di rilevamento, consultare la sezione [“Credenziali di rilevamento” a pagina 75](#).

Nota: Le credenziali possono essere preservate solo se il Discovery Manager è in esecuzione (stato verde).

3. Fare clic su **Ricrea database inventario**. Viene visualizzato il seguente messaggio di avvertenza - Eseguito questa azione si arresta temporaneamente il Discovery Manager. Ricreare il database inventario?

4. Fare clic su **OK** per ricreare il database inventario. Verrà visualizzato il seguente messaggio - Ricreazione database avviata. La ricreazione del database può richiedere approssimativamente 6 ore, nel frattempo viene visualizzato il seguente messaggio - dbinit in avvio nella pagina Riepilogo. Dopo 6 ore, è possibile controllare il **Log attività** per controllare se lo stato è Ricreazione database inventario riuscita.

Nota: Quando si ricrea il database inventario, il Discovery Manager si arresta temporaneamente e l'*Archivio ripulitura inventario* viene svuotato.

Esecuzione di RUNSTATS

Per eseguire il comando **RUNSTATS**, completare le seguenti operazioni:

1. Nel pannello di navigazione, fare clic su **Strumenti > Strumenti DB**.
2. Fare clic su **Esegui RUNSTATS**. Viene visualizzato il seguente messaggio di avvertenza - Eseguire RUNSTATS sulle tabelle di database dell'inventario?
3. Fare clic su **OK**. Verrà visualizzato il seguente messaggio - RUNSTATS avviato. Dopo circa 30 minuti, è possibile controllare il log attività. Al completamento del lavoro, il seguente messaggio viene aggiunto al log attività - RUNSTATS per il database inventario riuscito.

Esecuzione di REORG

Per eseguire il comando **REORG**, completare le seguenti operazioni:

1. Nel pannello di navigazione, fare clic su **Strumenti > Strumenti DB**.
2. Fare clic su **Esegui REORG**. Viene visualizzato il seguente messaggio di conferma - Eseguire REORG sulle tabelle di database dell'inventario?
3. Fare clic su **OK**. Il seguente messaggio viene aggiunto al log attività - REORG avviato. Dopo circa 30 minuti, è possibile controllare il log attività. Al completamento del lavoro, il seguente messaggio viene aggiunto al log attività - REORG per il database inventario riuscito.

Documentazione

Utilizzare la pagina **Documentazione** 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 TSA dal sito Web di TSA all'indirizzo: <https://ibm.biz/TSAdemo>.

Procedura

Per visualizzare la documentazione e acquisire maggiori informazioni su Technical Support Appliance, attenersi a questa procedura:

1. Fare clic su **Documentazione** dal menu di navigazione di sinistra.

Summary	<h1>IBM Technical Support Appliance (TSA) ?</h1>
Activity Log	
Inventory Summary	
Discovery Scopes	The IBM Technical Support Appliance (TSA) is an easy-to-use tool that enables you to get more value from your IBM Support contracts.
Discovery Credentials	
Discovery Schedule	
Discovery History	The link below will open a new web browser tab directly to the Technical Support Appliance information website on IBM.com. Here you will find everything you need to get started with IBM Technical Support Appliance. You can access setup guides and security documentation, view sample reports, and download the virtual appliance installation code from IBM Fix Central.
Discovery Settings	
Transmission Schedule	
Administration	Of special note, the Configuration Guide is a helpful index of best practices, tips, and shortcuts to configure TSA to efficiently retrieve IT device information from various hardware manufacturers.
Tools	
Documentation	Learn more about Technical Support Appliance: https://ibm.biz/TSAdemo
	 Technical Support Appliance Documentation

Figura 88. Documentazione

2. Per ulteriori informazioni su Technical Support Appliance, fare clic sul link: <https://ibm.biz/TSAdemo>
3. Sulla pagina **Installa TSA**, sono disponibili i link all'immagine TSA, alla guida di installazione, guida di configurazione e tutti i tutorial pertinenti.

Capitolo 7. Come contattare il supporto IBM per il TSA (Technical Support Appliance)

Il supporto IBM è disponibile dal lunedì al venerdì, nell'orario d'ufficio del proprio fuso orario.

Informazioni su questa attività

È possibile contattare il supporto IBM scegliendo una delle due seguenti opzioni:

1. [Aprire un caso su IBM Support Portal](#)
2. [Creare una richiesta di servizio tramite l'IBM Call Center](#)

Apertura di un caso su IBM Support Portal

Procedura

1. Accedere a <https://www.ibm.com/mysupport/s/>

Nota: È necessario creare un account prima di poter accedere a IBM Support Portal.

2. Fare clic su **Open a case** in alto a destra nel portale. Verrà visualizzata la pagina **Open a case**.
3. Selezionare **Type of support**.
4. Compilare i campi **Title**, **Product manufacturer** e **Product**.
Nota: Per instradare direttamente la richiesta al team di Technical Support Appliance, digitare **Technical Support Appliance** nel campo **Product**.
5. Selezionare un valore per **Severity**
6. Immettere una descrizione nel campo **Description** e selezionare la lingua preferita.
7. Se non è disponibile un operatore che parla la lingua desiderata e si desidera comunicare in inglese, selezionare **Yes**.
8. Fare clic su **Submit case**.

Creare una richiesta di servizio tramite l'IBM Call Center

Procedura

1. Comporre il numero di telefono corretto per il paese d'origine: <https://www.ibm.com/planetwide>
2. Selezionare la lingua.
3. Selezionare 1 (prodotti IBM).
4. Selezionare 2 (supporto software).
5. Utilizzare l'ID prodotto *5621IZX01* o il nome prodotto *Technical Support Appliance*.
6. Viene richiesto:
 - Numero azienda/area geografica
 - Nome cliente/azienda
 - Indirizzo/Città/Stato/Codice postale
 - Edificio/Piano/Stanza
 - Numero di telefono del luogo in cui si trova il TSA.
 - Nome di contatto/email/numero di telefono
 - Descrizione del problema

- Livello di severità

Appendice A. Installazione di TSA utilizzando il client VMware vSphere

Prima di iniziare

TSA richiede che sia caricato VMware ESXi 6.5, o versioni successive, per controllare l'hardware.

Informazioni su questa attività

Attenersi alla seguente procedura per installare l'immagine TSA. Per informazioni sui requisiti, consultare "Requisiti per TSA" a pagina 5.

Nota: La procedura (dal passo 1 al passo 12) è un esempio/riferimento della modalità di distribuzione dell'immagine di TSA. Alcuni di questi passi potrebbero variare in base alle procedure locali per la distribuzione delle macchine virtuali.

Procedura

Per installare TSA, attenersi alla seguente procedura:

1. Avviare il client VMware vSphere.
2. Accedere per stabilire una connessione al sistema ESXi.
3. Nel client vSphere, fare clic su **File > Distribuisci modello OVF**. Viene visualizzata la procedura guidata **Distribuisci modello OVF**.

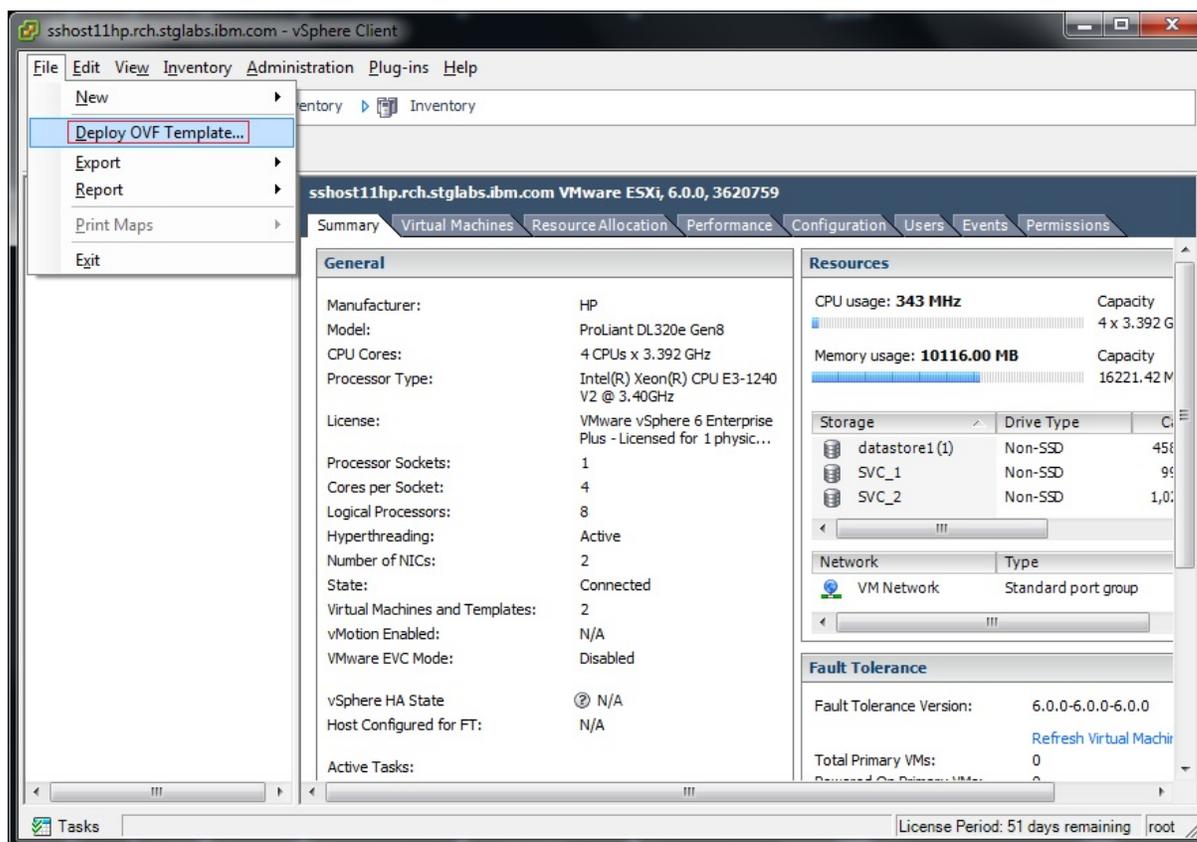


Figura 89. Distribuzione del modello OVF

4. Fare clic su **Sfoglia** e selezionare l'immagine salvata sul sistema.

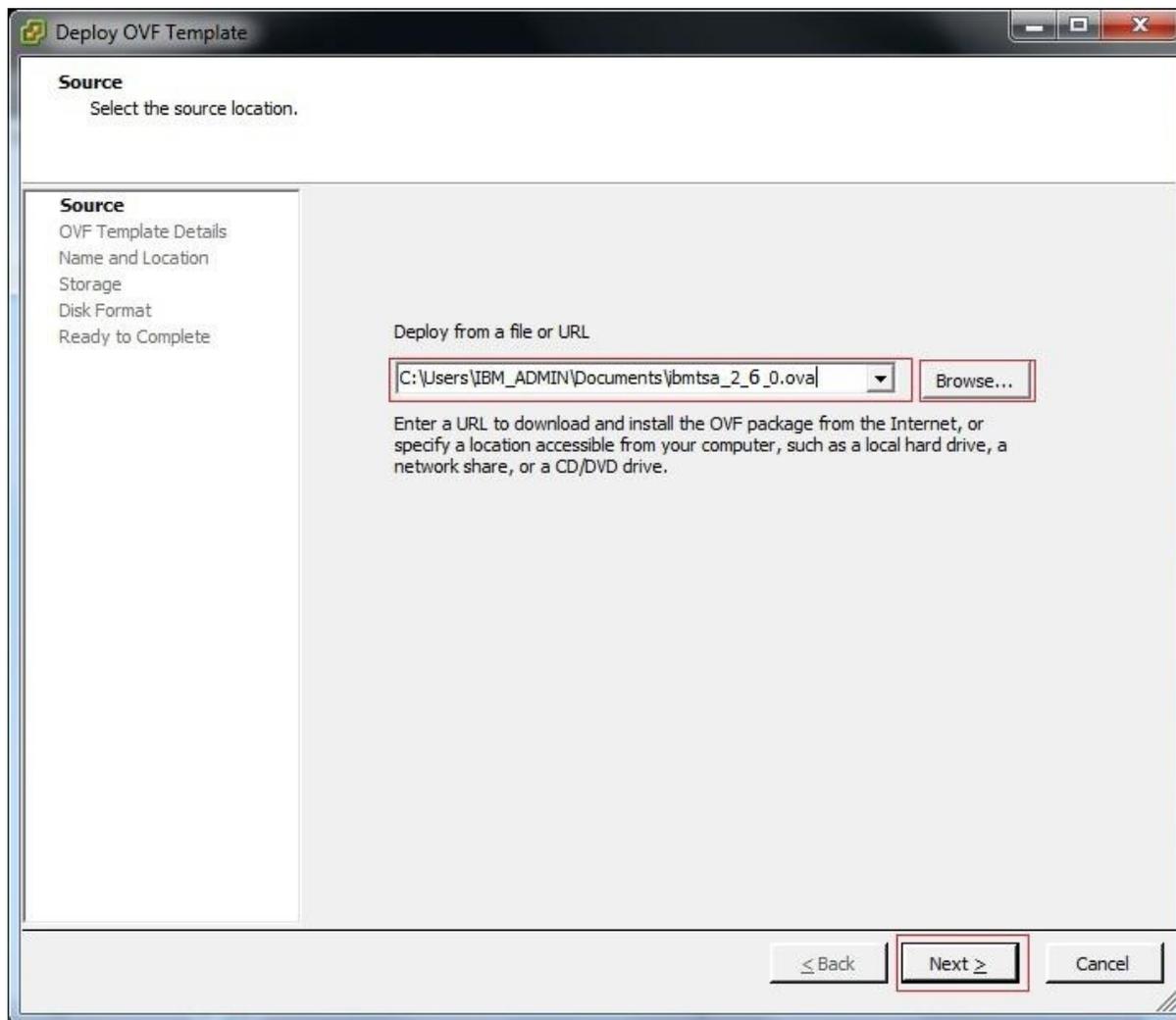


Figura 90. Origine del modello OVF

5. Fare clic su **Avanti**. Vengono visualizzati i **Dettagli del modello OVF**.
6. Fare clic su **Avanti**. Viene visualizzato il pannello **Nome e ubicazione**.

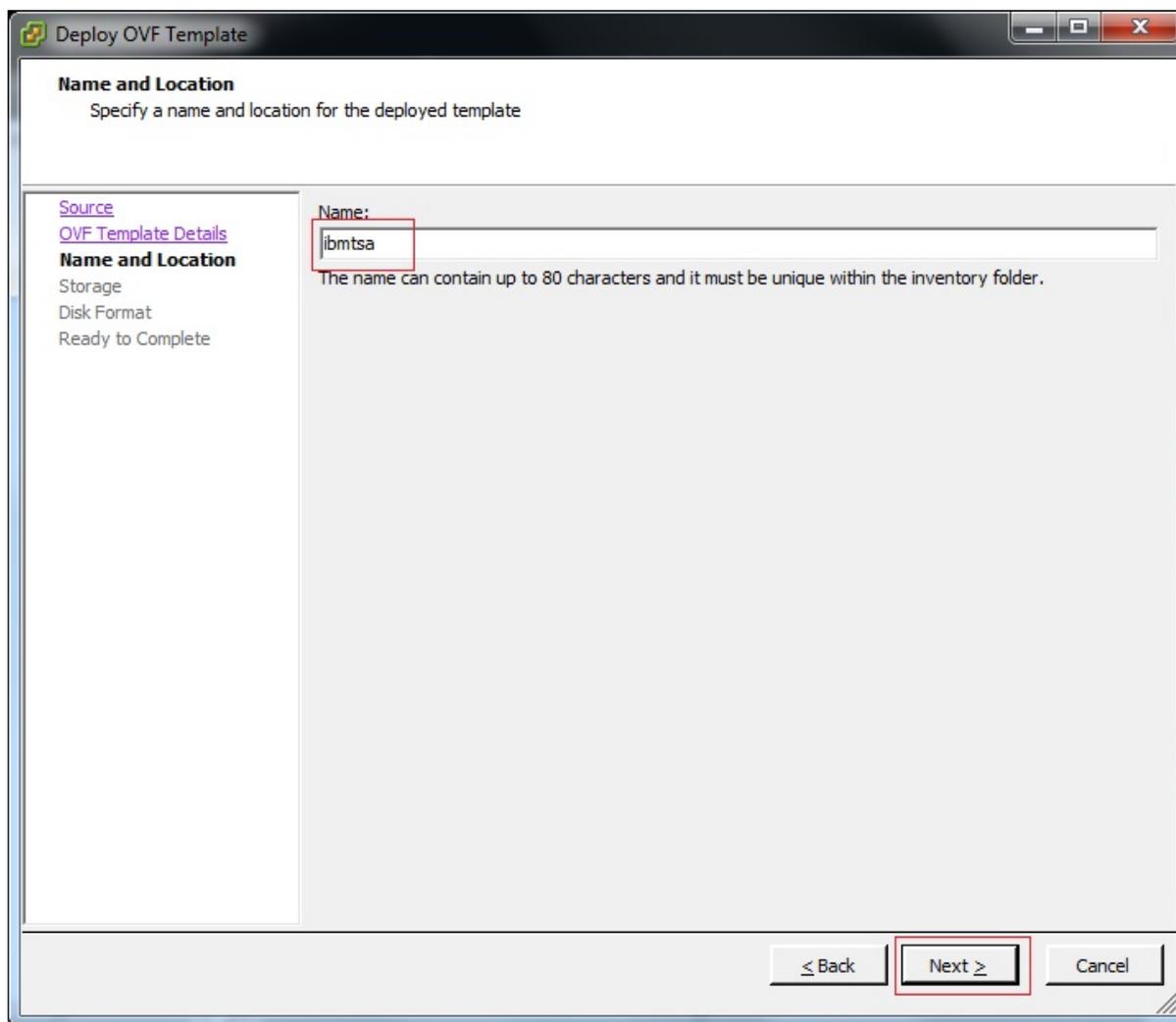


Figura 91. Nome e ubicazione

7. Nel pannello **Nome e ubicazione**, immettere il **Nome** per la macchina virtuale, oppure è possibile utilizzare il valore predefinito e fare clic su **Avanti**.
8. Nel pannello **Storage**, selezionare l'archivio dati (lo storage per i file della macchina virtuale) e fare clic su **Avanti**.

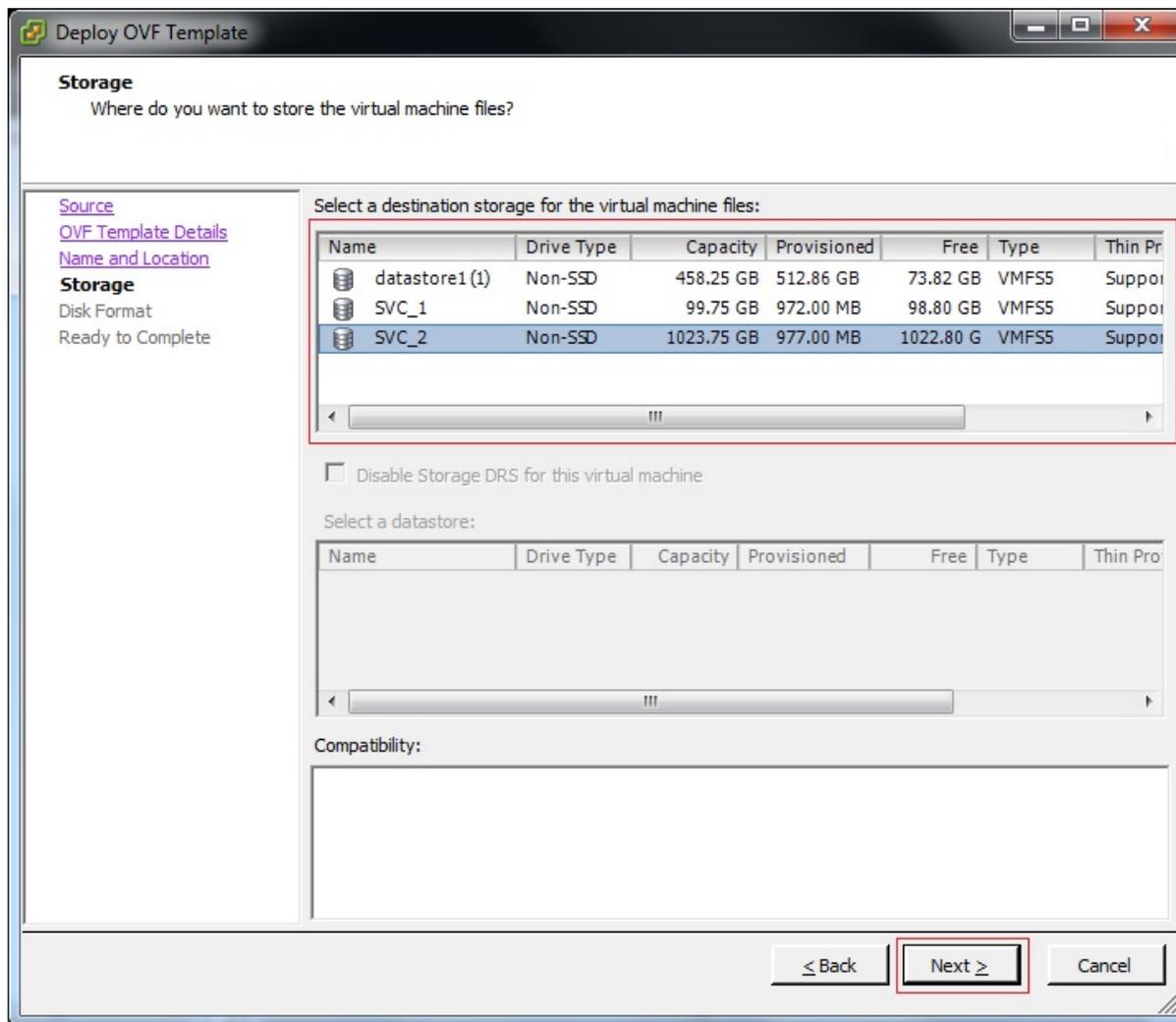


Figura 92. Storage

9. Nel pannello **Formato disco**, selezionare l'opzione **Thick Provision Eager Zeroed** e fare clic su **Avanti**.

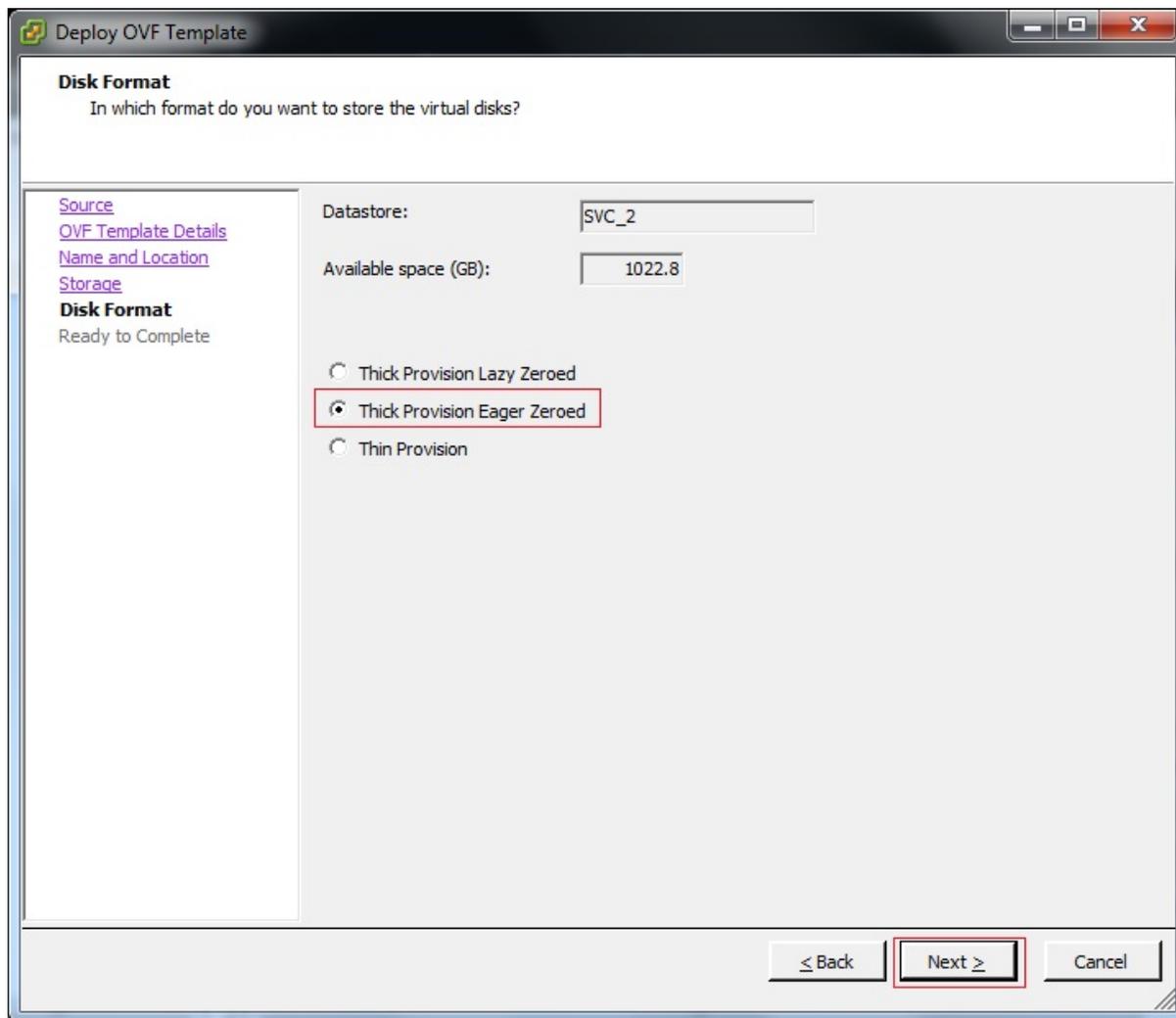


Figura 93. Formato disco

10. Se ESXi dispone di una sola connessione di rete, procedere al passo successivo. Altrimenti, selezionare la rete appropriata nel pannello **Associazione rete** e fare clic su **Avanti**.
11. Opzionale: Selezionare **Accendi dopo la distribuzione** per avviare automaticamente la macchina virtuale dopo la distribuzione. Inoltre, è possibile avviare manualmente la macchina virtuale dopo il completamento della distribuzione.

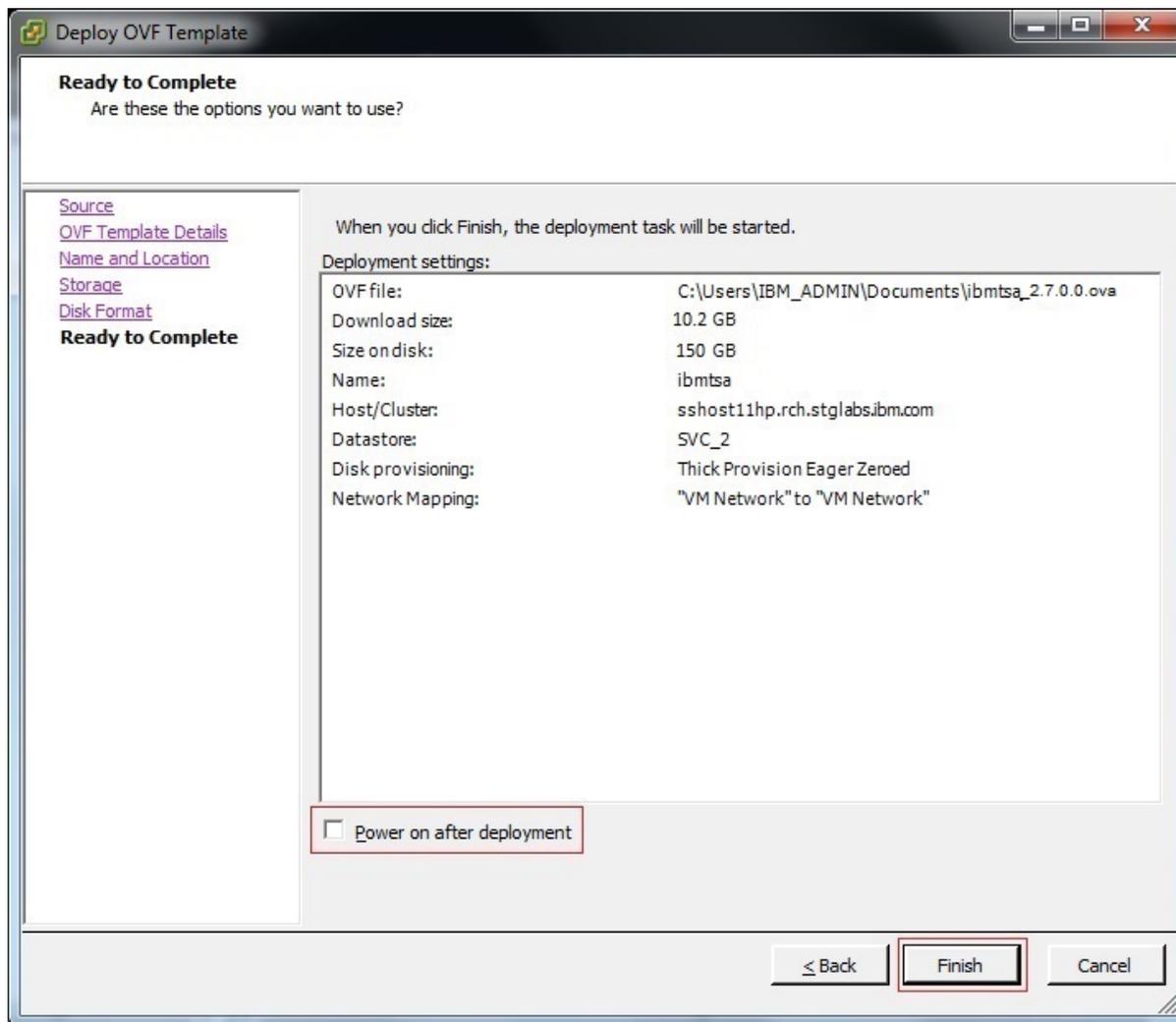


Figura 94. Pronto al completamento

12. Fare clic su **Finish**. La distribuzione di TSA potrebbe impiegare circa 30 minuti, ma questa stima potrebbe variare a seconda della velocità della connessione di rete tra il proprio sistema e il sistema VMware ESXi.
13. Una volta completata correttamente la distribuzione di TSA, selezionare la macchina virtuale appena distribuita e fare clic sulla scheda **Console** del client vSphere.
14. Accedere alla console di TSA per impostare la configurazione di rete. Immettere il valore di **ibmtsa login** come **tsausr** e **Password** come **configTsa**.
15. Richiesto: Per modificare la password di accesso, continuare con i passi elencati nella sezione “Modifica della password per tsaur (obbligatorio)” a pagina 19.
16. Per completare l'installazione, continuare con i passi elencati nella sezione “Configurazione dei dettagli di rete” a pagina 19.

Appendice B. Configurazione di Technical Support Appliance

Se si esce o si salta la configurazione di una delle impostazioni nella **procedura guidata di configurazione**, è possibile configurarle manualmente dal menu di navigazione a sinistra in TSA.

Registrazione di Technical Support Appliance

Registrazione delle informazioni sulle raccolte richieste per identificare TSA quando riporta informazioni a IBM per l'analisi.

Informazioni su questa attività

Per registrare TSA, attenersi alla seguente procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Registrazione**.
Viene visualizzata la pagina **Registrazione**.

- Summary
- Activity Log
- Inventory Summary
- Discovery Scopes
- Discovery Credentials
- Discovery Schedule
- Discovery History
- Discovery Settings
- Transmission Schedule
- Administration
 - Registration
 - License
 - Clock
 - Network
 - IBM Connectivity
 - User Accounts
 - Password
 - Security
 - Certificates
 - Backup and Restore
 - Update
 - Logging and Trace
 - Scheduled Maintenance
 - Data Snapshot
 - Shutdown
- Tools
- Documentation

Registration ?

This page allows you to view and change the system service contact and physical location information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Service Contact

Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

Company name: *
Name of the organization that owns or is responsible for this system.

Contact name:
Name of the person in your organization who is responsible for repairs and maintenance of the system.

Telephone number:
Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.

Email:
Email address of the contact person.

IBMid:
You can log on to the [IBM Client Insights Portal](#) with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to <https://www.ibm.com/account> to sign up.

System Location

Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.

Country or region: *
The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

State or province: *
The state or province where the system is located.

Postal code: *
The postal code where the system is located.

City: *
The city or locality where the system is located.

Street address: *
The first line of the system location address.

Telephone number:
The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.

Building, floor, office:
The building, floor, and office where the system is located.

➔ Save
✕ Cancel

Figura 95. Registrazione

2. Specificare le informazioni sul contatto di servizio nei seguenti campi:

Nome società

Il nome dell'organizzazione che utilizza TSA.

Nome contatto

(Facoltativo) Il nome della persona dell'organizzazione che è responsabile per TSA.

Numero di telefono

(Facoltativo) Il numero di telefono al quale può essere raggiunta la persona di contatto. Il numero di telefono deve includere il prefisso locale, il numero di scambio e l'interno. Non utilizzare le parentesi nei numeri di telefono.

Email

(Facoltativo) L'indirizzo email della persona di contatto.

IBMid

(Facoltativo) L'IBMid della persona che si desidera autorizzare a visualizzare i report su IBM Client Insights Portal.

Nota: È possibile accedere a <https://clientinsightsportal.ibm.com/> con il proprio IBMid associato per scaricare i report TSA in 1-2 giorni dopo ogni trasmissione di dati. Per registrarsi per un IBMid, andare all'indirizzo <https://www.ibm.com/account>.

Nota: Il contatto di servizio identifica la persona che il supporto IBM deve contattare se c'è un problema con il sistema. Le informazioni di contatto sono utilizzate per assistere IBM nel fornire all'azienda i risultati dell'analisi Technical Support Appliance.

3. Specificare le informazioni sull'ubicazione del TSA nei seguenti campi:

Paese o regione

Il paese o la regione in cui si trova il TSA.

Stato o provincia

Lo stato o la provincia in cui si trova il TSA. Se non si è certi dello Stato, immettere *Sconosciuto*

Codice postale

Il codice postale relativo all'ubicazione del TSA.

Città

La città o località in cui si trova il TSA.

Indirizzo

L'indirizzo dell'ubicazione del TSA.

Numero di telefono

(Facoltativo) Il numero di telefono della stanza in cui si trova il TSA. Il numero di telefono deve includere il prefisso locale, il numero di scambio e l'interno. Non utilizzare le parentesi nei numeri di telefono.

Edificio, piano, ufficio

(Facoltativo) L'edificio, il piano e l'ufficio in cui si trova il TSA.

4. Fare clic su **Salva** per salvare le informazioni di registrazione.

Configurazione della connettività IBM

Specificare le informazioni sulla connessione Internet da utilizzare per la connessione a IBM.

Prima di iniziare

Assicurarsi che il firewall consenta le connessioni al nome host e agli indirizzi IP del server IBM, come spiegato in [Tabella 1 a pagina 6](#). Se la rete non consente l'accesso ai server IBM, le transazioni di TSA al supporto IBM avranno esito negativo.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Connettività IBM**.

Figura 96. Connettività IBM

2. Nel pannello **Accesso**, effettuare la selezione tra i seguenti tipi di accesso Internet:

Consenti connessione SSL diretta

TSA si connette a IBM mediante connessione diretta.

Utilizza connessione proxy SSL

TSA si connette IBM mediante connessione proxy SSL.

Utilizza connessione proxy SSL di autenticazione

TSA si connette a IBM mediante una connessione proxy SSL di autenticazione.

3. Se è stato selezionato **Utilizza connessione proxy SSL** o **Utilizza connessione proxy SSL di autenticazione**, specificare le seguenti informazioni per il server proxy.

Indirizzo IP o nome host

L'indirizzo IP o il nome host del server proxy.

Nota: Il nome host immesso non deve contenere caratteri di sottolineatura ("_").

Porta

Il numero di porta del server proxy.

4. Se è stato selezionato **Utilizza connessione proxy SSL di autenticazione**, specificare le seguenti informazioni per il server proxy:

Nome utente

Il nome utente che il server proxy richiede per l'autenticazione.

Password

La password associata al nome utente che il server proxy richiede per l'autenticazione.

Conferma password

Reimmettere la password. Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.

5. Fare clic su **Salva** per salvare le informazioni di connessione a IBM.
6. Fare clic su **Verifica connessione** per verificare la connessione specificata.

Importante:

- Salvare le impostazioni di connessione prima di verificare la connessione.
- È necessario avere una connessione funzionante a IBM o le funzioni TSA non funzioneranno.

Concetti correlati

Requisiti di configurazione per le connessioni al Supporto IBM

TSA può connettersi al supporto IBM tramite connessione diretta o tramite un proxy fornito dall'utente che deve essere configurato in modo da consentire la comunicazione con IBM. Se si utilizza un proxy, l'ispezione TLS/SSL non è supportata. Alle richieste tramite un proxy deve essere consentito di fluire direttamente a IBM senza terminazione TLS/SSL.

Impostazione dell'orologio

È necessario impostare l'ora, la data e il fuso orario locale del sistema TSA durante la configurazione.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Orologio**.
Viene visualizzata la pagina **Orologio**.

Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
 Registration
 License
Clock
 Network
 IBM Connectivity
 User Accounts
 Password
 Security
 Certificates
 Backup and Restore
 Update
 Logging and Trace
 Scheduled Maintenance
 Data Snapshot
 Shutdown
Tools
Documentation

Clock

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Time Zone

Define the Greenwich Mean Time (GMT) offset corresponding to the time zone where this system is located and whether the system clock should automatically adjust when Daylight Savings Time (DST) changes.

GMT offset: *

DST adjustment: *

Select Time Option

Select whether to use a local or public NTP (Network Time Protocol) server to update the system clock automatically or manually configure it.

Select: *

Date and Time

Manually set the system date and time.

Date (mm/dd/yyyy): *
 Defines the manually set system date.

Time (hh:mm:ss): *
 Defines the manually set system time.

NTP Settings

Defines the IP addresses or hostnames of up to 2 Network Time Protocol servers for system clock synchronization.

NTP server 1: *
 Defines the IP address or hostname for NTP server 1.

NTP server 2:
 Defines the IP address or hostname for NTP server 2.

Figura 97. Orologio

2. Selezionare il fuso orario locale dall'elenco a discesa **Differenza GMT**.
3. Selezionare l'adattamento dell'ora legale (o DST - daylight saving time) dall'elenco a discesa **Modifica DST**.

Nota: Non tutti i fusi orari consentono l'ora legale. Se si seleziona questa opzione per un fuso orario che non consente l'ora legale, viene visualizzato un errore.

4. Selezionare un metodo per aggiornare l'orologio di sistema dall'elenco a discesa **Seleziona opzione ora**.

Le opzioni includono la sincronizzazione dell'orologio di sistema con un server NTP (Network Time Protocol) per aggiornare automaticamente l'orologio di sistema o configurarlo manualmente.

- a) Se si sceglie di configurare manualmente l'orologio di sistema, è necessario impostare la data e l'ora del sistema. Immettere le informazioni di data e ora nei campi **Data e Ora**.
- b) Se si sceglie di sincronizzare l'orologio di sistema con un server NTP (Network Time Protocol) per aggiornare automaticamente l'orologio di sistema, è necessario specificare gli indirizzi IP e i nomi host dei server NTP. Immettere le informazioni per indirizzo IP o nome host per un massimo di due server nei campi **Server NTP**.

Nota: Assicurarsi che il server NTP sia accessibile tramite la rete per TSA.

5. Fare clic su **Salva** per salvare le informazioni sull'orologio.

Risultati

Nota: Alcune modifiche richiedono il riavvio per diventare effettive. Ad esempio, se è stata impostata la data o l'ora, o si passa dalla configurazione manuale alla configurazione del server NTP, viene richiesto di riavviare il server.

Configurazione della pianificazione della trasmissione

TSA fornisce una pianificazione predefinita in base alla quale eseguire il processo di trasmissione a un determinato orario. È possibile modificare questa pianificazione in base alle esigenze.

Procedura

1. Nel pannello di navigazione, fare clic su **Pianificazione trasmissione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Il pannello **Pianifica** visualizza la successiva esecuzione pianificata e l'ora. Il pannello **Cronologia** visualizza lo stato e ulteriori dettagli dei lavori di trasmissione correntemente in esecuzione e precedenti.

2. Fare clic su **Modifica pianificazione**.

Viene visualizzata la pagina **Pianificazione trasmissione**.

Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Documentation

Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule
Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission

Schedule
Select when you want the transmission performed.

At hour: * 00
At minute: * 00

Day selection mode: *
 Weekly by day(s) (Sun-Sat)
 Monthly by date(s) (1-31)

On days: *
 01 02 03 04 05 06 07
 08 09 10 11 12 13 14
 15 16 17 18 19 20 21
 22 23 24 25 26 27 28
 29 30 31

If days are picked beyond the last day of any given month, the job will be triggered the last day of such month instead.

Save Cancel

Figura 98. Modifica della pianificazione della trasmissione

- a) Utilizzare gli elenchi a discesa **A ore** e **A minuti** per selezionare il nuovo orario.
- b) Selezionare **Modalità di selezione giorno**.

Per giorno settimanale (dom-sab)

Per pianificare la trasmissione in giorni specifici di una settimana, selezionare l'opzione **Per giorno settimanale (dom-sab)**.

Schedule

Select when you want the transmission performed.

At hour: *

At minute: *

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Figura 99. Per giorno settimanale (dom-sab)

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni della settimana.

Per data mensile (1-31)

Per pianificare la trasmissione in giorni specifici di un mese, selezionare l'opzione **Mensilmente per giorni (1-31)**.

Per il campo **Nei giorni**, selezionare la casella di spunta appropriata per scegliere uno o più giorni del mese.

Nota: Se si selezionano giorni oltre l'ultimo giorno di un mese specifico, il lavoro verrà attivato l'ultimo giorno di tale mese.

3. Fare clic su **Salva**.

Viene visualizzata di nuovo la pagina **Pianificazione trasmissione** con la nuova pianificazione.

Aggiornamento

È possibile controllare la disponibilità di aggiornamenti per TSA e scaricarli.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Aggiorna**.

Viene visualizzata la pagina **Aggiornamento**.

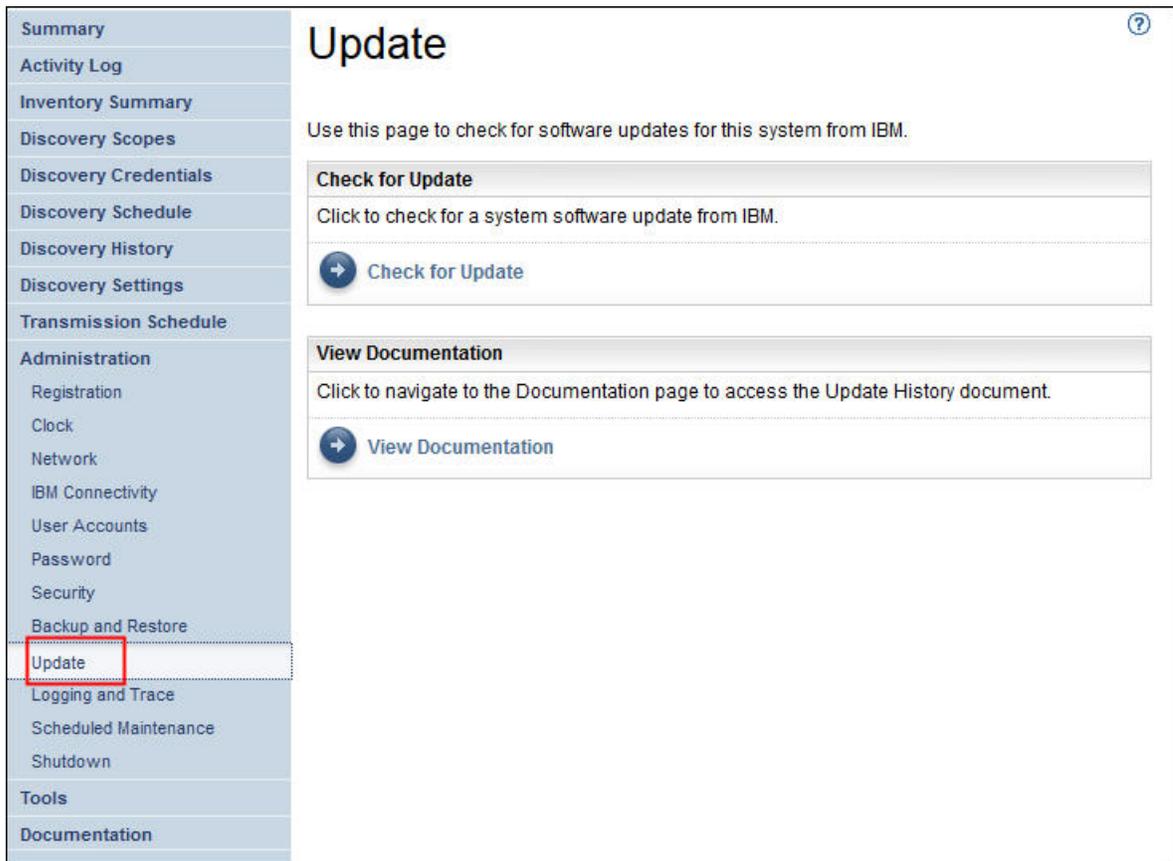


Figura 100. Aggiornamento

2. Fare clic su **Controlla aggiornamenti**.

La pagina **Disponibilità degli aggiornamenti** elenca gli eventuali aggiornamenti disponibili.

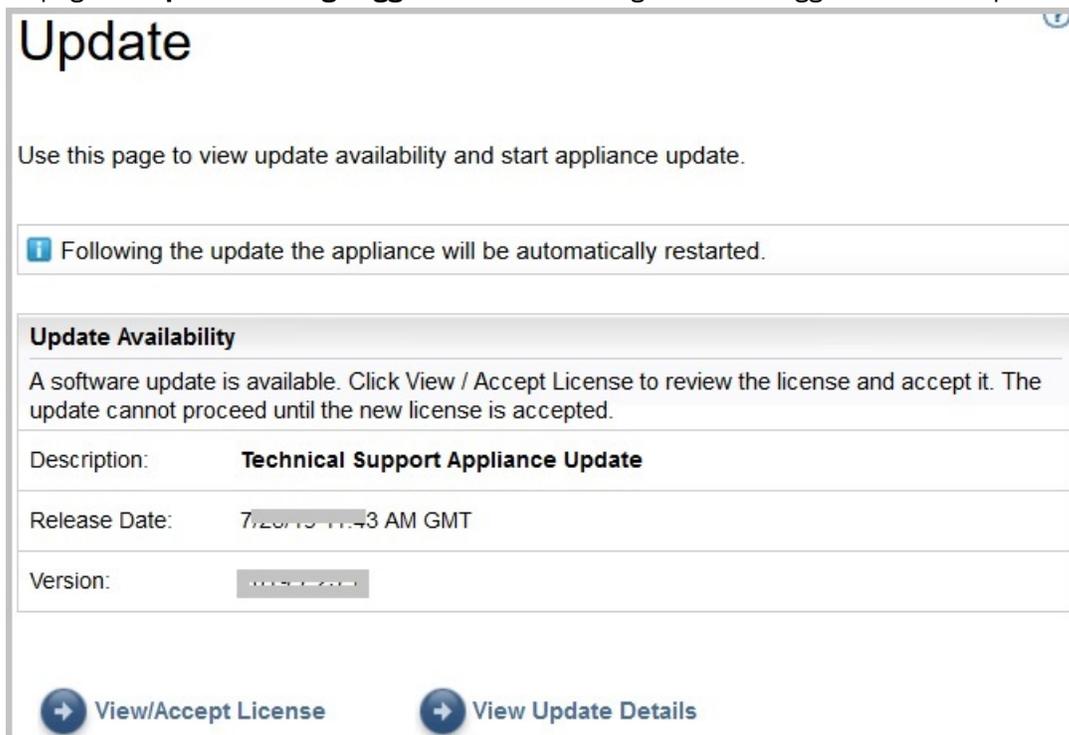


Figura 101. Disponibilità degli aggiornamenti

- a) Per alcune nuove release di TSA, è necessario accettare un nuovo accordo di licenza prima di procedere con l'aggiornamento. Se esiste una nuova licenza, fare clic su **Visualizza/Accepta licenza**; verrà visualizzata la pagina **Accordo di licenza**.
- b) Fare clic sul pulsante **Accetta** sulla pagina **Accordo di licenza** per accettare il nuovo accordo di licenza. Viene visualizzata nuovamente la pagina **Aggiornamento** con il pulsante **Esegui ora l'aggiornamento**. Se non è richiesto di accettare un nuovo accordo di licenza, non viene visualizzato il pulsante **Visualizza/Accepta licenza** ed è possibile procedere facendo clic sul pulsante **Esegui ora l'aggiornamento**.

Nota:

- Una volta accettata la licenza, non viene più visualizzato il pulsante **Visualizza/Accepta licenza**.
 - Nel pannello di navigazione, fare clic su **Amministrazione > Licenza** per visualizzare l'Accordo di licenza più recente accettato.
- c) Per installare gli aggiornamenti, fare clic su **Esegui ora l'aggiornamento**.

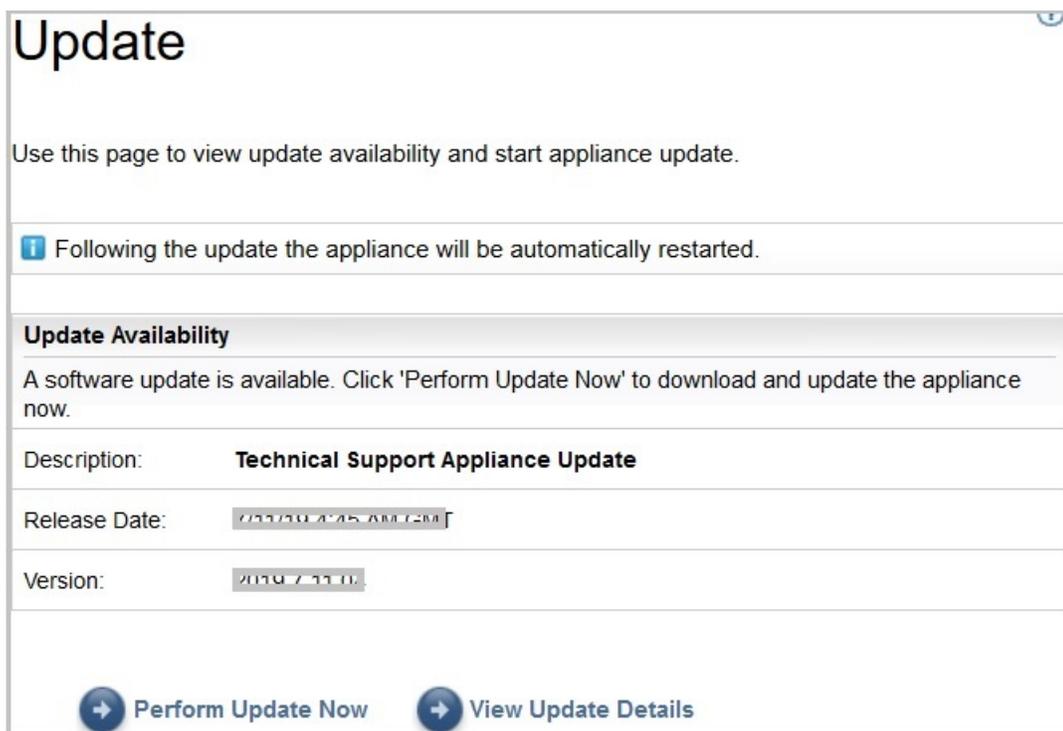


Figura 102. Esegui ora l'aggiornamento

Una volta completato l'aggiornamento, TSA viene riavviato automaticamente.

- d) Per visualizzare le informazioni relative ai contenuti dell'aggiornamento, fare clic su **Visualizza dettagli dell'aggiornamento**.

Appendice C. Configurazione dei dettagli di rete DHCP

Attenersi alla seguente procedura per configurare i dettagli di rete DHCP:

Procedura

1. Selezionare l'opzione **1) Impostazione della configurazione di rete** dal **menu di configurazione TSA**.

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option:
```

Figura 103. Impostazione della configurazione di rete

2. Immettere i seguenti dettagli della configurazione di rete.

```
Enter IPTYPE={static|dhcp}:dhcp
Enter Hostname(default=ibmtsa):ibmappliance
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:dhcp
HOSTNAME:ibmappliance
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:
```

Figura 104. Configurazione di rete

- a) **Immettere IPTYPE = {static|dhcp}**. Immettere dhcp.

IPTYPE: dhcp

Immettere il nome host (valore predefinito=ibmtsa). È possibile modificare il nome host predefinito. Assicurarsi che il nome host utilizzato sia univoco.

Immettere il dominio di rete del sistema per l'utilizzo DNS (facoltativo).

Immettere DNS 1 (facoltativo), Immettere DNS 2 (facoltativo) e Immettere DNS 3 (facoltativo).

I dettagli della configurazione di rete specificati vengono visualizzati per la conferma.

- b) Immettere **[y|n]** per confermare o eliminare la configurazione di rete. Immettendo **y**, la configurazione di rete viene salvata e il sistema viene riavviato automaticamente.

Nota: Per le eventuali configurazioni non corrette, è possibile modificare i dettagli. Immettere **n** per ignorare le impostazioni correnti e riavviare la configurazione dal passo “2.a” a pagina 135

- c) Affinché la nuova configurazione di rete abbia effetto, il sistema viene riavviato dopo 15 secondi.
- d) Dopo il riavvio del sistema, accedere al virtualization manager e annotare l'**Indirizzo IP** sulla scheda **Riepilogo**.

The screenshot displays the VMware vSphere interface for a virtual machine named 'ibmtsa_2.7.0.0'. The interface is divided into several sections:

- General Information:** Shows the host name 'sshot10hptsa', IP addresses '10.10.10.10' (highlighted with a red box), VMware Tools status (Installed: Yes, Version: 10240, Running: Yes), and Storage (1 disk).
- Hardware Configuration:** Lists 4 vCPUs, 16 GB Memory, 150 GB Hard disk 1, VM Network (Connected) Network adapters, Remote Floppy 0, 8 MB Video card, and Remote ATAPI CD/DVD drive 0.
- Resource Consumption:** Shows 42 MHz Consumed host CPU, 3.69 GB Consumed host memory, and 6.24 GB Active guest memory.
- Storage:** Shows 150 GB Provisioned, 147.39 GB Uncommitted, 169.99 GB Not-shared, and 169.99 GB Used.

A performance summary graph is also visible at the bottom left, showing 'Consumed host CPU' (green), 'Ready' (blue), and 'Consumed host memory...' (dark blue) over time.

Figura 105. Indirizzo IP DHCP

- e) Accedere a TSA dal browser con l'URL ottenuto nel passo precedente. Ad esempio, <https://newhost1.new.abclabs.example.com>

Nota: Durante la prima connessione, il browser potrebbe visualizzare un'eccezione di sicurezza. È necessario accettare il certificato di sicurezza e proseguire con l'accesso a TSA.

Appendice D. Account utente e gruppi di utenti

È possibile utilizzare gli account utente e i gruppi di utenti per concedere l'accesso alle funzioni di TSA.

Prima di iniziare

TSA è installato con un account utente denominato **admin**. Questo account dispone dell'autorizzazione di eseguire qualsiasi funzione di TSA. È possibile che si vogliono aggiungere account utente per le seguenti ragioni:

- Consentire ad un altro utente di fungere da backup per l'utente **admin**.
- Consentire ad alcuni utenti di accedere ad una quantità limitata di funzioni su TSA.

Informazioni su questa attività

L'esecuzione di qualsiasi funzione di TSA richiede un certo livello di autorizzazione. Se un utente autenticato tenta di eseguire una funzione senza il livello di autorizzazione appropriato, viene visualizzato un errore e la funzione non viene eseguita.

In TSA i livelli di autorizzazione sono associati ai gruppi di utenti. Agli utenti vengono assegnate le appartenenze a uno o più gruppi di utenti e, tramite tali appartenenze, gli utenti hanno il livello di autorizzazione per eseguire funzioni particolari.

TSA viene fornito con un gruppo utenti **Amministratore** e un account utente **admin**. Il gruppo utenti **Amministratore** dispone di accesso illimitato a tutte le funzioni del sistema. L'account utente **admin** viene assegnato al gruppo utenti **Amministratore**.

Visualizzazione di account utente e gruppi di utenti

È possibile visualizzare account utente e gruppi di utenti esistenti.

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Account utente**.

Viene visualizzata la pagina **Account utente e gruppi**.

2. Per visualizzare gli account utente esistenti, fare clic sulla scheda **Account**.

La tabella Account utente mostra gli account utente.

Suggerimento: Per visualizzare i dettagli per un account utente specifico, fare clic sul nome dell'account utente. Il pannello **Generale** visualizza il nome utente, il nome completo e la descrizione associata all'account utente selezionato. Fare clic sul pannello **Membro di** sulla destra, per visualizzare i gruppi di utenti a cui appartiene questo account utente.

3. Per visualizzare i gruppi di utenti esistenti, fare clic sulla scheda **Gruppi**.

La tabella Gruppi di utenti mostra i gruppi di utenti.

Suggerimento: Per visualizzare i dettagli per un gruppo di utenti specifico, fare clic sul nome del gruppo di utenti. Il pannello **Generale** visualizza il nome e il livello di autorizzazione associati al gruppo di utenti. Fare clic sul pannello **Limitazioni ambito** sulla destra, per visualizzare le serie di ambiti che il gruppo di utenti selezionato può rilevare. Fare clic sul pannello **Membri** per visualizzare gli account utente associati a questo gruppo di utenti.

Aggiunta di account utente e gruppi di utenti

È possibile aggiungere account utente e gruppi di utenti per controllare l'accesso alle funzioni di TSA.

Concetti correlati

Ambiti di rilevamento e Serie di ambiti

Gli ambiti di rilevamento identificano le risorse che si desidera che TSA rilevi. Gli ambiti di rilevamento sono raggruppati in serie di ambiti di rilevamento.

Aggiunta di un gruppo di utenti

È possibile aggiungere gruppi di utenti per controllare l'accesso alle funzioni di TSA.

Informazioni su questa attività

Per aggiungere un gruppo di utenti, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione** > **Account utente**.
Viene visualizzata la pagina **Account utente e gruppi**.
2. Fare clic sulla scheda **Gruppi**.

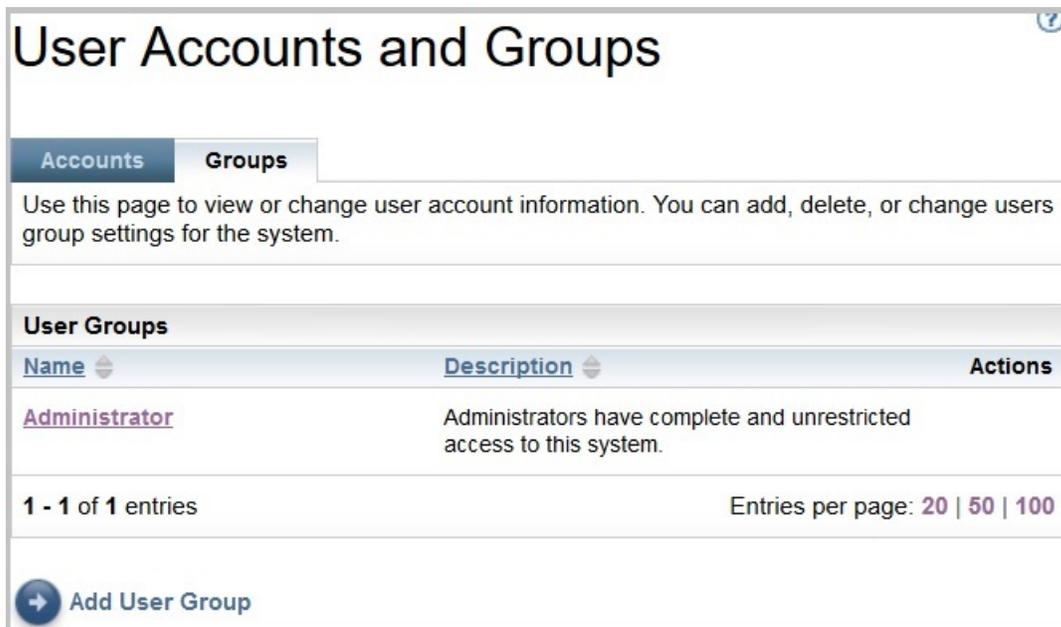


Figura 106. Gruppi

3. Fare clic su **Aggiungi gruppo di utenti**.
Viene visualizzata la pagina **Gruppo di utenti**.

User Group

Use this page to view, add or change user group information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user group basic information.

Group name: *	<input type="text" value="Test"/> <small>Uniquely identifies the group.</small>
Description:	<input type="text" value="Testing"/> <small>Describes the group.</small>

Member Authority Level

All members of this group will have the following authority level.

Select: *

Restrict To Selected Scope Sets

Identifies the scope sets this group is restricted to.

Scope set name:	<input type="checkbox"/> AIX_Scope <input type="checkbox"/> AIX_Scope_TADDM <input type="checkbox"/> AMM_Scope <input type="checkbox"/> Test <input type="checkbox"/> Test_IPRange_ScopeSet <input type="checkbox"/> Tester1 <input type="checkbox"/> WindowsScopeSet <input type="checkbox"/> XIV_Scope
------------------------	---

Figura 107. Aggiungi gruppo di utenti

4. Nel campo **Nome gruppo**, immettere un nome univoco per il gruppo.
5. Opzionale: Nel campo **Descrizione**, immettere una descrizione per questo gruppo di utenti.
6. Selezionare il livello di autorizzazione che si desidera abbiano i membri del gruppo di utenti.
TSA definisce i seguenti livelli di autorizzazione gruppo:
 - **Amministratore** – nessuna limitazione
 - **Rilevamento** – solo funzioni di rilevamento
 - **Visitatore** – accesso di sola lettura
7. Se si specifica il livello di autorizzazione *Rilevamento* per questo gruppo di utenti, è necessario selezionare almeno una serie di ambiti limitata a questo gruppo di utenti.
Per maggiori informazioni sulle serie di ambiti, consultare [“Ambiti di rilevamento e Serie di ambiti” a pagina 1.](#)
8. Fare clic su **Salva** per salvare il gruppo di utenti.

Viene visualizzata la pagina **Account utente e gruppi** con il nuovo gruppo di utenti nell'elenco.

Aggiunta di un account utente

È possibile aggiungere account utente per controllare l'accesso alle funzioni di TSA.

Informazioni su questa attività

Per aggiungere un account utente, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Account utente**.

Viene visualizzata la pagina **Account utente e gruppi**.

User ID	Full Name	Description	Password Age	Actions	
1	admin	Administrator	All Jobs	Temporary	
2	Tester	Tester1	Perform Testing	Temporary	

Figura 108. Account utente e gruppi

2. Per definire un nuovo account utente, fare clic su **Aggiungi account utente**.

Viene visualizzata la pagina **Account utente**.

User Account ?

Use this page to view, add or change user account information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: *	<input type="text" value="James"/> <small>Uniquely identifies the user.</small>
Full name:	<input type="text" value="Robert"/> <small>Identifies the users full name.</small>
Description:	<input type="text" value="Developer"/> <small>Describes the user.</small>

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password: *	<input type="password" value="••••••••"/>
Confirm new password: *	<input type="password" value="••••••••"/>
Disable Account:	<input type="checkbox"/> Account is disabled

Member Of

The groups this user is a member of.

Select user groups: *	<input type="checkbox"/> VisitorGroup-ForTest <input checked="" type="checkbox"/> Administrator
------------------------------	--

Figura 109. Aggiungi account utente

3. Nel campo **Nome utente**, immettere un nome per questo account utente.
4. Opzionale: Nel campo **Nome completo**, immettere un nome completo per l'utente di questo account.
5. Opzionale: Nel campo **Descrizione**, immettere una descrizione per questo account utente.
6. Nel campo **Nuova password**, immettere una password per questo account utente.

La password deve rispettare le seguenti regole:

- Deve essere lunga almeno 8 caratteri
 - Deve contenere almeno un carattere alfabetico e un carattere non alfabetico
 - Non deve contenere il nome utente
 - Non deve essere uguale a una delle precedenti otto password
 - Deve essere modificata almeno una volta ogni 30 giorni (per impostazione predefinita) o, come specificato nella sezione [“Modifica della durata della password”](#) a pagina 104, ma non dovrà essere modificata più di una volta al giorno.
7. Nel campo **Conferma password**, immettere nuovamente la password per questo account utente.
Le due password immesse vengono confrontate perché corrispondano, prima che venga salvata la password.

Nota: La password deve essere modificata al primo accesso a questo account utente.

8. Se si desidera disabilitare questo account utente, selezionare la casella di spunta **L'account è disabilitato**.

La disabilitazione dell'account permette di impedire che l'account sia utilizzato, senza dover eliminare l'account.

Nota: Non è possibile disabilitare l'account **amministratore** né modificare il gruppo dell'account **amministratore**.

9. Selezionare i gruppi di utenti per questo account utente. È necessario selezionare almeno un gruppo di utenti. L'utente avrà il livello di autorizzazione definito per qualsiasi gruppo si seleziona.
10. Fare clic su **Salva** per salvare l'account utente.
Viene visualizzata la pagina **Account utente e gruppi** con il nuovo account utente nell'elenco.

Modifica di account utente e gruppi di utenti

È possibile modificare account utente e gruppi di utenti esistenti.

Modifica di account utente

È possibile modificare account utente esistenti.

Informazioni su questa attività

Per modificare un account utente, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Account utente**.
Viene visualizzata la pagina **Account utente e gruppi**.
2. Fare clic sulla scheda **Account**, quindi sull'icona **Modifica**  accanto all'account utente.
Viene visualizzata la pagina **Account utente**.
3. Nel pannello **Generale**, è possibile modificare le impostazioni di base per questo account utente.
4. Nel pannello **Immettere la password**, è possibile modificare la password e le informazioni di gestione della password. È anche possibile disabilitare questo account utente.

La password deve rispettare le seguenti regole:

- Deve essere lunga almeno 8 caratteri
- Deve contenere almeno un carattere alfabetico e un carattere non alfabetico
- Non deve contenere il nome utente
- Non deve essere uguale a una delle precedenti otto password
- Deve essere modificata almeno una volta ogni 90 giorni, ma non deve essere modificata più di una volta al giorno

Nota: La password deve essere modificata al primo accesso a questo account utente.

5. Se si desidera disabilitare questo account utente, selezionare **L'account è disabilitato**.

La disabilitazione dell'account permette di impedire che l'account sia utilizzato, senza dover eliminare l'account. Per informazioni sull'eliminazione di un account utente, consultare [“Eliminazione di account utente e gruppi di utenti”](#) a pagina 144.

Nota: Non è possibile disabilitare l'account **amministratore** né modificare il gruppo dell'account **amministratore**.

User Account

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: *
Uniquely identifies the user.

Full name:
Identifies the user's full name.

Description:
Describes the user.

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password:

Confirm new password:

Disable Account: Account is disabled

Member Of

The groups this user is a member of.

Select user groups: * Administrator

Figura 110. Modificare l'account utente admin

- Nel pannello **Membro di**, è possibile modificare i gruppi di utenti a cui appartiene questo account utente. L'account utente deve essere membro di almeno un gruppo di utenti:
- Fare clic su **Salva** per salvare le modifiche.
Le informazioni modificate vengono visualizzate nella pagina **Account utente e gruppi**.

Modifica di gruppi di utenti

È possibile modificare i gruppi di utenti esistenti.

Prima di iniziare

Nota: Non è possibile modificare il gruppo **Amministratore**.

Informazioni su questa attività

Per modificare un gruppo di utenti, attenersi a questa procedura:

Procedura

- Nel pannello di navigazione, fare clic su **Amministrazione** > **Account utente**.
Viene visualizzata la pagina **Account utente e gruppi**.
- Fare clic sulla scheda **Gruppi**, quindi sull'icona **Modifica**  accanto al gruppo di utenti.
Viene visualizzata la pagina **Gruppo di utenti**.
- Nel pannello **Generale**, è possibile modificare le impostazioni di base per questo gruppo di utenti.
- Nel pannello **Livello di autorizzazione membro**, è possibile modificare se questo gruppo di utenti ha l'autorizzazione *Amministratore*, *Rilevamento* o *Lettura*.

5. Se si specifica il livello di autorizzazione *Rilevamento* in **Livello di autorizzazione membro**, è possibile modificare le serie di ambiti per cui questo gruppo di utenti ha l'autorizzazione di rilevamento nel pannello **Limita alle serie di ambiti selezionate**.
6. Fare clic su **Salva** per salvare le modifiche.
Le informazioni modificate vengono visualizzate nella pagina **Account utente e gruppi**.

Eliminazione di account utente e gruppi di utenti

È possibile eliminare account utente e gruppi di utenti esistenti.

Eliminazione di account utente

È possibile eliminare gli account utente

Informazioni su questa attività

Nota: L'account utente **admin** non può essere eliminato.

Per eliminare un account utente, attenersi a questa procedura:

Procedura

1. Nel pannello di navigazione, fare clic su **Amministrazione > Account utente**.
Viene visualizzata la pagina **Account utente e gruppi**.
2. Fare clic sulla scheda **Account**, quindi sull'icona Elimina  accanto all'account utente che si desidera eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare l'account utente.

Eliminazione di gruppi di utenti

È possibile eliminare i gruppi di utenti esistenti.

Informazioni su questa attività

Nota: Il gruppo di utenti **Amministratore** non può essere eliminato.

Per eliminare un gruppo di utenti, attenersi a questa procedura:

Procedura

1. Fare clic su **Amministrazione > Account utente**.
Viene visualizzata la pagina **Account utente e gruppi**.
2. Fare clic sulla scheda **Gruppi**, quindi sull'icona Elimina  accanto all'account utente che si desidera eliminare.
3. Fare clic su **OK** per confermare che si desidera eliminare il gruppo di utenti.

Nota: Un gruppo di utenti può essere eliminato solo se a esso non sono assegnati utenti.

Accessibilità

Technical Support Appliance non interferisce con le funzioni di accessibilità per i browser supportati. Per un elenco completo delle funzioni di accessibilità, visitare la pagina del supporto all'accessibilità per il browser supportato che si sta utilizzando. Per un elenco dei browser supportati, consultare [“Browser web richiesti”](#) a pagina 5.

Le pubblicazioni per questo prodotto sono nel formato Adobe Portable Document Format (PDF) e devono essere conformi agli standard di accessibilità. Se si riscontrano difficoltà durante l'utilizzo dei file PDF e si desidera richiedere un formato basato su web per una pubblicazione, inviare una richiesta tramite email al seguente indirizzo:

icfeedback@us.ibm.com

In alternativa, è possibile spedire una richiesta al seguente indirizzo:

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

Nella richiesta, accertarsi di includere il titolo della pubblicazione, "Guida alla configurazione di Technical Support Appliance" nell'oggetto della lettera.

Quando si inviano informazioni a IBM, si concede a IBM il diritto non esclusivo di utilizzare o distribuire le informazioni nel modo che IBM ritiene appropriato senza incorrere in alcun obbligo nei confronti dell'utente.

Note legali

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

IBM può non offrire i prodotti, i servizi o le funzioni presentati in questo documento in altri paesi. Consultare il proprio rappresentante locale IBM per informazioni sui prodotti ed i servizi attualmente disponibili nella propria zona. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica o intende dichiarare che solo quel prodotto, programma o servizio IBM può essere utilizzato. Qualsiasi prodotto funzionalmente equivalente al prodotto, programma o servizio che non violi alcun diritto di proprietà intellettuale IBM può essere utilizzato. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura del presente documento non concede alcuna licenza a tali brevetti. È possibile inviare per iscritto richieste di licenze a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali: LA IBM (INTERNATIONAL BUSINESS MACHINES CORPORATION) FORNISCE LA PRESENTE PUBBLICAZIONE NELLO STATO IN CUI SI TROVA, SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, MA NON LIMITATE A, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIALIZZABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia ad alcune garanzie espresse o implicite in determinate transazioni, pertanto, la presente dichiarazione può non essere applicabile.

Queste informazioni potrebbero includere inesattezze tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. IBM può effettuare miglioramenti e/o modifiche ai prodotti e/o ai programmi descritti nella presente pubblicazione in qualsiasi momento senza preavviso.

Qualsiasi riferimento in queste informazioni a siti Web non IBM sono fornite solo per convenienza e non servono in alcun modo da approvazione di tali siti Web. I materiali presenti in tali siti Web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti Web è a proprio rischio.

IBM può utilizzare o distribuire qualsiasi informazione fornita in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo verso l'utente.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono notevolmente variare. Alcune misurazioni possono essere state effettuate su sistemi del livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate tramite estrapolazione. I risultati reali possono variare. Gli utenti del presente documento dovranno verificare i dati applicabili per i propri ambienti specifici.

Le informazioni relative a prodotti non IBM sono ottenute dai fornitori di quei prodotti, dagli annunci pubblicati e da altre fonti disponibili al pubblico. IBM non ha testato quei prodotti e non può confermarne l'accuratezza della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Le domande sulle capacità dei prodotti non IBM dovranno essere indirizzate ai fornitori di tali prodotti.

Tutte le dichiarazioni relative all'orientamento e alle intenzioni future di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo mete e obiettivi.

Queste informazioni sono solo per scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Marchi

IBM, il logo IBM e ibm.com sono marchi o marchi registrati di International Business Machines Corp., registrati in molte giurisdizioni di tutto il mondo. Altri nomi di prodotti e servizi potrebbero essere marchi di IBM o di altre società. Un elenco attuale di marchi IBM è disponibile sul Web nella sezione "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" all'indirizzo www.ibm.com/legal/copytrade.shtml.

Linux è un marchio di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft, Windows, Hyper-V e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Java™ e tutti i marchi e i logo basati su Java sono marchi o marchi registrati di Oracle e/o delle sue affiliate.

VMware, il logo VMware, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server e VMware vSphere sono marchi o marchi registrati di VMware, Inc. o delle sue affiliate negli Stati Uniti e/o in altre giurisdizioni.



Numero parte:

(1P) P/N: