Monitorare le porte di rete

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/networking/monitor_the_health_of_network_ports.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommario

Monitorare le porte di rete

Monitorare lo stato delle porte di rete

La gestione ONTAP delle porte di rete include il monitoraggio automatico dello stato di salute e un set di monitor per aiutare a identificare le porte di rete che potrebbero non essere adatte per l'hosting di LIF.

A proposito di questa attività

Se un monitor dello stato di salute determina che una porta di rete non è funzionante, avvisa gli amministratori tramite un messaggio EMS o contrassegna la porta come danneggiata. ONTAP evita l'hosting di LIF su porte di rete degradate se sono presenti destinazioni di failover alternative sane per tale LIF. Una porta può diventare degradata a causa di un errore di tipo soft, come ad esempio il link flapping (link che rimbalzano rapidamente tra up e down) o la partizione di rete:

- Le porte di rete nell'IPSpace del cluster vengono contrassegnate come degradate quando si verificano lo sfarfallio del collegamento o la perdita di raggiungibilità Layer 2 (L2) ad altre porte di rete nel dominio di trasmissione.
- Le porte di rete negli spazi IP non cluster vengono contrassegnate come degradate quando si verifica lo sfarfallio dei collegamenti.

È necessario conoscere i seguenti comportamenti di una porta danneggiata:

- Una porta degradata non può essere inclusa in una VLAN o in un gruppo di interfacce.

  Se una porta membro di un gruppo di interfacce è contrassegnata come degradata, ma il gruppo di interfacce è ancora contrassegnato come integro, i file LIF possono essere ospitati su quel gruppo di interfacce.

- Le LIF vengono migrate automaticamente dalle porte degradate alle porte integre.
- Durante un evento di failover, una porta degradata non viene considerata come destinazione di failover. Se non sono disponibili porte integre, le porte degradate ospitano le LIF in base alla normale policy di failover.
- Non è possibile creare, migrare o ripristinare una LIF su una porta degradata.

  È possibile modificare `ignore-health-status` impostazione della porta di rete su `true`. È quindi possibile ospitare una LIF sulle porte sane.

Fasi

1. Accedere alla modalità avanzata dei privilegi:

   ```
   set -privilege advanced
   ```

2. Controllare quali monitor di stato sono abilitati per il monitoraggio dello stato delle porte di rete:

   ```
   network options port-health-monitor show
   ```

   Lo stato di salute di una porta è determinato dal valore dei monitor di stato.

I seguenti monitor di stato sono disponibili e abilitati per impostazione predefinita in ONTAP:

- Monitor di stato link-flapping: Monitora il link flapping

  Se una porta presenta uno sfarfallio del collegamento più di una volta in cinque minuti, questa porta viene contrassegnata come degradata.

- L2 Reachability Health Monitor: Monitora se tutte le porte configurate nello stesso dominio di trasmissione hanno una raggiungibilità L2 l'una rispetto all'altra

  Questo monitor dello stato di salute segnala problemi di raggiungibilità L2 in tutti gli spazi IP; tuttavia, contrassegna solo le porte nell'IPSpace del cluster come degradate.

- Monitor CRC: Monitora le statistiche CRC sulle porte

  Questo monitor dello stato di salute non contrassegna una porta come degradata, ma genera un messaggio EMS quando si osserva un tasso di guasti CRC molto elevato.

3. Attivare o disattivare i monitor di stato di un IPSpace come desiderato utilizzando `network options port-health-monitor modify` comando.
4. Visualizzazione dello stato dettagliato di una porta:

```
network port show -health
```

L'output del comando visualizza lo stato di salute della porta, `ignore health status` impostazione ed elenco dei motivi per cui la porta è contrassegnata come degradata.

Lo stato di integrità della porta può essere `healthy` oppure `degraded`.

Se il `ignore health status` l'impostazione è `true`, indica che lo stato di salute della porta è stato modificato da `degraded` a. `healthy` dall'amministratore.

Se il `ignore health status` l'impostazione è `false`, lo stato delle porte viene determinato automaticamente dal sistema.

Monitorare la raggiungibilità delle porte di rete (ONTAP 9,8 e versioni successive)

Il monitoraggio della raggiungibilità è integrato in ONTAP 9.8 e versioni successive. Utilizzare questo monitoraggio per identificare quando la topologia fisica della rete non corrisponde alla configurazione ONTAP. In alcuni casi, ONTAP può riparare la raggiungibilità delle porte. In altri casi, sono necessari ulteriori passaggi.

A proposito di questa attività

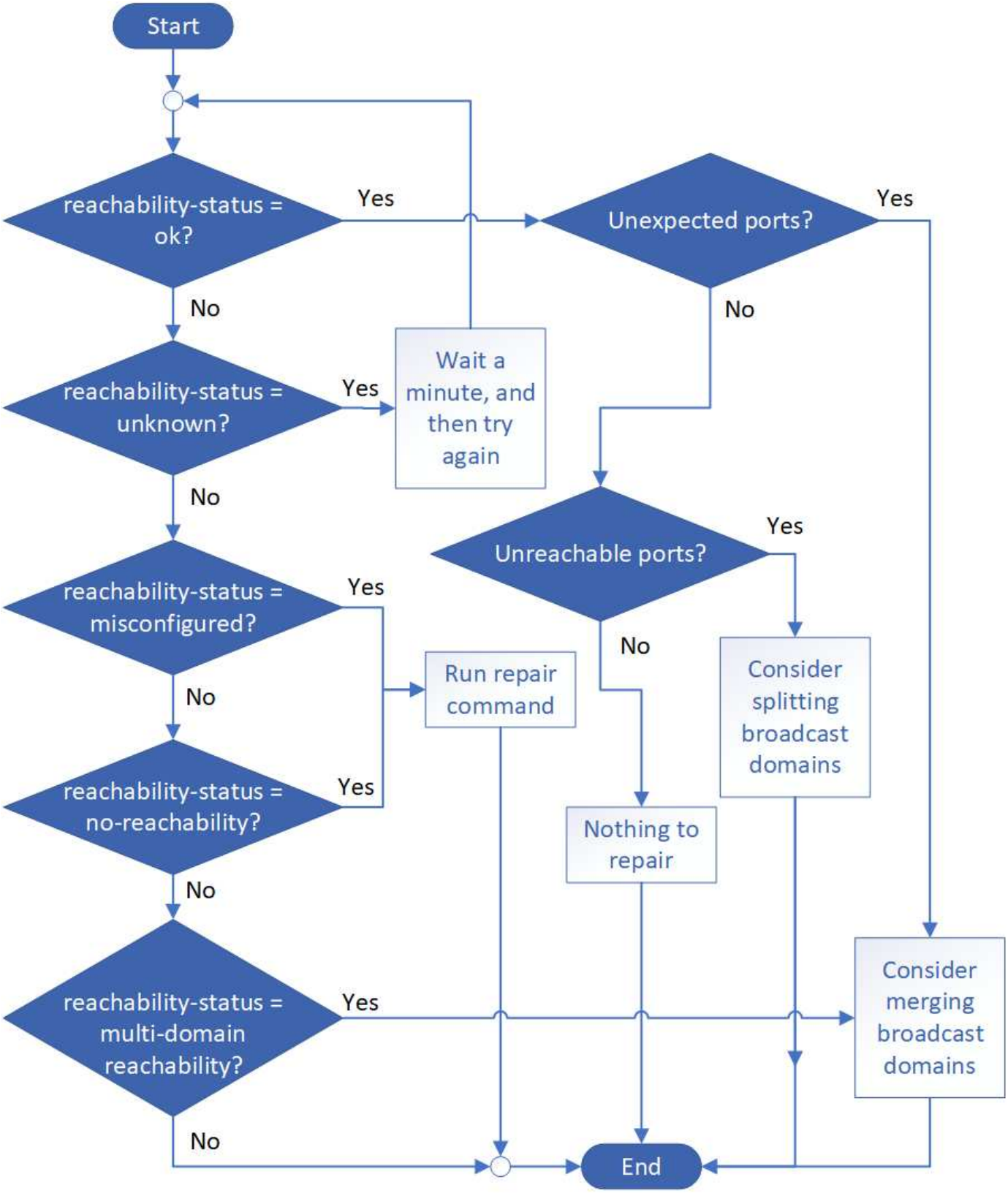
Utilizzare questi comandi per verificare, diagnosticare e riparare le configurazioni errate della rete derivanti dalla configurazione ONTAP che non corrisponde al cablaggio fisico o alla configurazione dello switch di rete.

Fase

1. Visualizzazione della raggiungibilità delle porte:

```
network port reachability show
```

2. Utilizzare la seguente struttura decisionale e la seguente tabella per determinare la fase successiva, se presente.



Stato di raggiungibilità	Descrizione
ok	La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato. Se lo stato di raggiungibilità è "ok", ma ci sono "porte impreviste", considerare la possibilità di unire uno o più domini di broadcast. Per ulteriori informazioni, consulta la seguente riga *Unexpected ports*. Se lo stato di raggiungibilità è "ok", ma ci sono "porte irraggiungibili", considerare la possibilità di suddividere uno o più domini di broadcast. Per ulteriori informazioni, consultare la riga *Unreachable ports* riportata di seguito. Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.
Porte impreviste	La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast. Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione. Per ulteriori informazioni, vedere "Unire i domini di broadcast".
Porte non raggiungibili	Se un singolo dominio di broadcast è stato suddiviso in due diversi set di raggiungibilità, è possibile suddividere un dominio di broadcast per sincronizzare la configurazione ONTAP con la topologia fisica della rete. In genere, l'elenco delle porte irraggiungibili definisce il set di porte che devono essere suddivise in un altro dominio di trasmissione dopo aver verificato che la configurazione fisica e quella dello switch sono accurate. Per ulteriori informazioni, vedere "Suddividere i domini di broadcast".
riconfigurazione non corretta	La porta non dispone di capacità di livello 2 rispetto al dominio di trasmissione assegnato; tuttavia, la porta dispone di capacità di livello 2 rispetto a un dominio di trasmissione diverso. È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta al dominio di trasmissione a cui è possibile accedere: `network port reachability repair -node -port`Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte".

nessuna raggiungibilità	La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente. È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta a un nuovo dominio di trasmissione creato automaticamente in IPSpace predefinito: `network port reachability repair -node -port`Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte".
raggiungibilità multi-dominio	La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast. Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione. Per ulteriori informazioni, vedere "Unire i domini di broadcast" oppure "Riparare la raggiungibilità delle porte".
sconosciuto	Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.

Dopo aver riparato una porta, è necessario controllare e risolvere le LIF e le VLAN spostate. Se la porta faceva parte di un gruppo di interfacce, è necessario comprendere anche cosa è successo a quel gruppo di interfacce. Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte".

Panoramica delle porte ONTAP

Alcune porte note sono riservate per le comunicazioni ONTAP con servizi specifici. I conflitti di porta si verificano se il valore di una porta nell'ambiente di rete dello storage è lo stesso della porta ONTAP.

La seguente tabella elenca le porte TCP e UDP utilizzate da ONTAP.

Servizio	Porta/protocollo	Descrizione
ssh	22/TCP	Login shell sicuro
telnet	23/TCP	Accesso remoto
DNS	53/TCP	DNS con bilanciamento del carico
http	80/TCP	Hyper Text Transfer Protocol
rpcbind	111/TCP	Chiamata di procedura remota
rpcbind	111/UDP	Chiamata di procedura remota
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC

netbios-sn	139/TCP	Sessione del servizio NetBIOS
snmp	161/UDP	Protocollo di gestione di rete semplice
https	443/TCP	HTTP su TLS
microsoft-ds	445/TCP	Microsoft-ds
montare	635/TCP	Montaggio NFS
montare	635/UDP	Montaggio NFS
con nome	953/UDP	Nome daemon
nfs	2049/UDP	Daemon del server NFS
nfs	2049/TCP	Daemon del server NFS
nrv	2050/TCP	Protocollo NetApp Remote Volume
iscsi	3260/TCP	Porta di destinazione iSCSI
blocco	4045/TCP	Daemon di blocco NFS
blocco	4045/UDP	Daemon di blocco NFS
NSM	4046/TCP	Network Status Monitor (Monitor di stato della rete
NSM	4046/UDP	Network Status Monitor (Monitor di stato della rete
rquotad	4049/UDP	Protocollo NFS rquotad
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS - protocollo binario di ascolto
https	8443/TCP	7MTT GUI Tool tramite https
ndmp	10000/TCP	Network Data Management Protocol
Peering dei cluster	11104/TCP	Peering dei cluster, bidirezionale
Peering dei cluster, bidirezionale	11105/TCP	Peering dei cluster
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	accetta connessioni di controllo su prese sicure
porta del testimone cifs	40001/TCP	porta del testimone cifs
tls	50000/TCP	Sicurezza del livello di trasporto
iscsi	65200/TCP	Porta ISCSI

Porte interne ONTAP

La tabella seguente elenca le porte TCP e UDP utilizzate internamente da ONTAP. Queste porte vengono utilizzate per stabilire una comunicazione LIF intracluster:

Porta/protocollo	Descrizione

514	Syslog
900	RPC cluster di NetApp
902	RPC cluster di NetApp
904	RPC cluster di NetApp
905	RPC cluster di NetApp
910	RPC cluster di NetApp
911	RPC cluster di NetApp
913	RPC cluster di NetApp
914	RPC cluster di NetApp
915	RPC cluster di NetApp
918	RPC cluster di NetApp
920	RPC cluster di NetApp
921	RPC cluster di NetApp
924	RPC cluster di NetApp
925	RPC cluster di NetApp
927	RPC cluster di NetApp
928	RPC cluster di NetApp
929	RPC cluster di NetApp
931	RPC cluster di NetApp
932	RPC cluster di NetApp
933	RPC cluster di NetApp
934	RPC cluster di NetApp
935	RPC cluster di NetApp
936	RPC cluster di NetApp
937	RPC cluster di NetApp
939	RPC cluster di NetApp
940	RPC cluster di NetApp
951	RPC cluster di NetApp
954	RPC cluster di NetApp
955	RPC cluster di NetApp
956	RPC cluster di NetApp
958	RPC cluster di NetApp
961	RPC cluster di NetApp
963	RPC cluster di NetApp

964	RPC cluster di NetApp
966	RPC cluster di NetApp
967	RPC cluster di NetApp
982	RPC cluster di NetApp
983	RPC cluster di NetApp
5125	Porta di controllo alternativa per il disco
5133	Porta di controllo alternativa per il disco
5144	Porta di controllo alternativa per il disco
65502	SSH. Ambito nodo
65503	Condivisione LIF
7810	RPC cluster di NetApp
7811	RPC cluster di NetApp
7812	RPC cluster di NetApp
7813	RPC cluster di NetApp
7814	RPC cluster di NetApp
7815	RPC cluster di NetApp
7816	RPC cluster di NetApp
7817	RPC cluster di NetApp
7818	RPC cluster di NetApp
7819	RPC cluster di NetApp
7820	RPC cluster di NetApp
7821	RPC cluster di NetApp
7822	RPC cluster di NetApp
7823	RPC cluster di NetApp
7824	RPC cluster di NetApp
8023	Ambito del nodo TELNET
8514	Scope del nodo RSH
9877	Porta client KMIP (solo host locale interno)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.