Überwachen Sie die Netzwerkanschlüsse

ONTAP 9

NetApp
April 24, 2024

Inhalt

Überwachen Sie die Netzwerkanschlüsse

Überwachen Sie den Systemzustand von Netzwerk-Ports

Das ONTAP Management von Netzwerk-Ports umfasst eine automatische Statusüberwachung und eine Reihe von Zustandsmonitoren, mit denen Sie Netzwerk-Ports identifizieren können, die möglicherweise nicht für das Hosting von LIFs geeignet sind.

Über diese Aufgabe

Wenn eine Systemzustandsüberwachung feststellt, dass ein Netzwerkanschluss fehlerhaft ist, werden Administratoren über eine EMS-Meldung gewarnt oder der Port wird als beeinträchtigt markiert. ONTAP vermeidet das Hosten von LIFs auf beeinträchtigten Netzwerk-Ports, wenn es gesunde alternative Failover-Ziele für diese LIF gibt. Ein Port kann aufgrund eines Soft-Failure-Ereignisses beeinträchtigt werden, z. B. das Überfüllen von Links (die schnell zwischen oben und unten hin- und herspringt) oder die Netzwerkpartitionierung:

- Netzwerkanschlüsse im IPspace des Clusters werden als beeinträchtigt markiert, wenn es zu Verbindungsverlusten oder Verlust der Reachabilität von Layer 2 (L2) zu anderen Netzwerkports in der Broadcast-Domäne kommt.
- Netzwerkports in nicht-Cluster-IPspaces werden als beeinträchtigt gekennzeichnet, wenn Link-flattern.

Sie müssen die folgenden Verhaltensweisen eines beeinträchtigten Ports kennen:

- Ein eingeschränkter Port kann nicht in ein VLAN oder eine Schnittstellengruppe aufgenommen werden.

  Wenn ein Mitglied-Port einer Interface-Gruppe als beeinträchtigt gekennzeichnet ist, die Interface-Gruppe jedoch noch als ordnungsgemäß gekennzeichnet ist, können LIFs auf dieser Interface-Gruppe gehostet werden.

- LIFs werden automatisch von Ports migriert, deren Betrieb nicht beeinträchtigt ist, auf gesunde Ports.
- Während eines Failover-Ereignisses wird ein beeinträchtigter Port nicht als Failover-Ziel betrachtet. Wenn keine ordnungsgemäßen Ports verfügbar sind, hosten degradierte Ports LIFs gemäß der normalen Failover-Richtlinie.
- Sie können eine LIF nicht zu einem beeinträchtigten Port erstellen, migrieren oder zurücksetzen.

  Sie können den ändern `ignore-health-status` Einstellen des Netzwerkports auf `true`. Sie können dann eine LIF auf den gesunden Ports hosten.

Schritte

1. Melden Sie sich im erweiterten Berechtigungsmodus an:

   ```
   set -privilege advanced
   ```

2. Überprüfen Sie, welche Integritätsmonitore für das Monitoring des Netzwerkports aktiviert sind:

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

Der Integritätsstatus eines Ports wird durch den Wert der Integritätsmonitore bestimmt.

Die folgenden Integritätsmonitore sind in ONTAP standardmäßig verfügbar und aktiviert:

- Link-flatternder Systemzustandsüberwachung: Überwacht das Umfüllen von Links

  Wenn ein Port in fünf Minuten mehr als einmal über Verbindungsflattern verfügt, wird dieser Port als beeinträchtigt markiert.

- L2-Statusüberwachung: Überwacht, ob alle Ports, die in derselben Broadcast-Domäne konfiguriert sind, L2-Erreichbarkeit aufweisen

  Diese Systemzustandsüberwachung meldet Probleme mit der L2-Erreichbarkeit in allen IPspaces. Es markiert jedoch nur die Ports im Cluster-IPspace als beeinträchtigt.

- CRC-Monitor: Überwacht die CRC-Statistiken auf den Ports

  Diese Systemzustandsüberwachung markiert einen Port nicht als beeinträchtigt, generiert aber eine EMS-Meldung, wenn eine sehr hohe CRC-Fehlerrate beobachtet wird.

3. Aktivieren oder deaktivieren Sie eine der Integritätsmonitore für einen IPspace nach Bedarf mithilfe des `network options port-health-monitor modify` Befehl.
4. Anzeigen des detaillierten Systemzustands eines Ports:

```
network port show -health
```

In der Ausgabe des Befehls wird der Systemzustand des Ports angezeigt, `ignore health status` Einstellung und eine Liste der Gründe, warum der Port als beeinträchtigt gekennzeichnet ist.

Ein Port-Integritätsstatus kann sein `healthy` Oder `degraded`.

Wenn der `ignore health status` Einstellung lautet `true`, Zeigt an, dass der Status des Ports von geändert wurde `degraded` Bis `healthy` Vom Administrator.

Wenn der `ignore health status` Einstellung lautet `false`, Der Zustand des Ports wird automatisch vom System ermittelt.

Überwachung der Erreichbarkeit von Netzwerkports (ONTAP 9.8 und höher)

Die Überwachung der Erreichbarkeit ist in ONTAP 9.8 und höher integriert. Mithilfe dieses Monitoring wird ermittelt, ob die physische Netzwerktopologie nicht mit der ONTAP Konfiguration übereinstimmt. In einigen Fällen kann ONTAP die Erreichbarkeit des Ports reparieren. In anderen Fällen sind weitere Schritte erforderlich.

Über diese Aufgabe

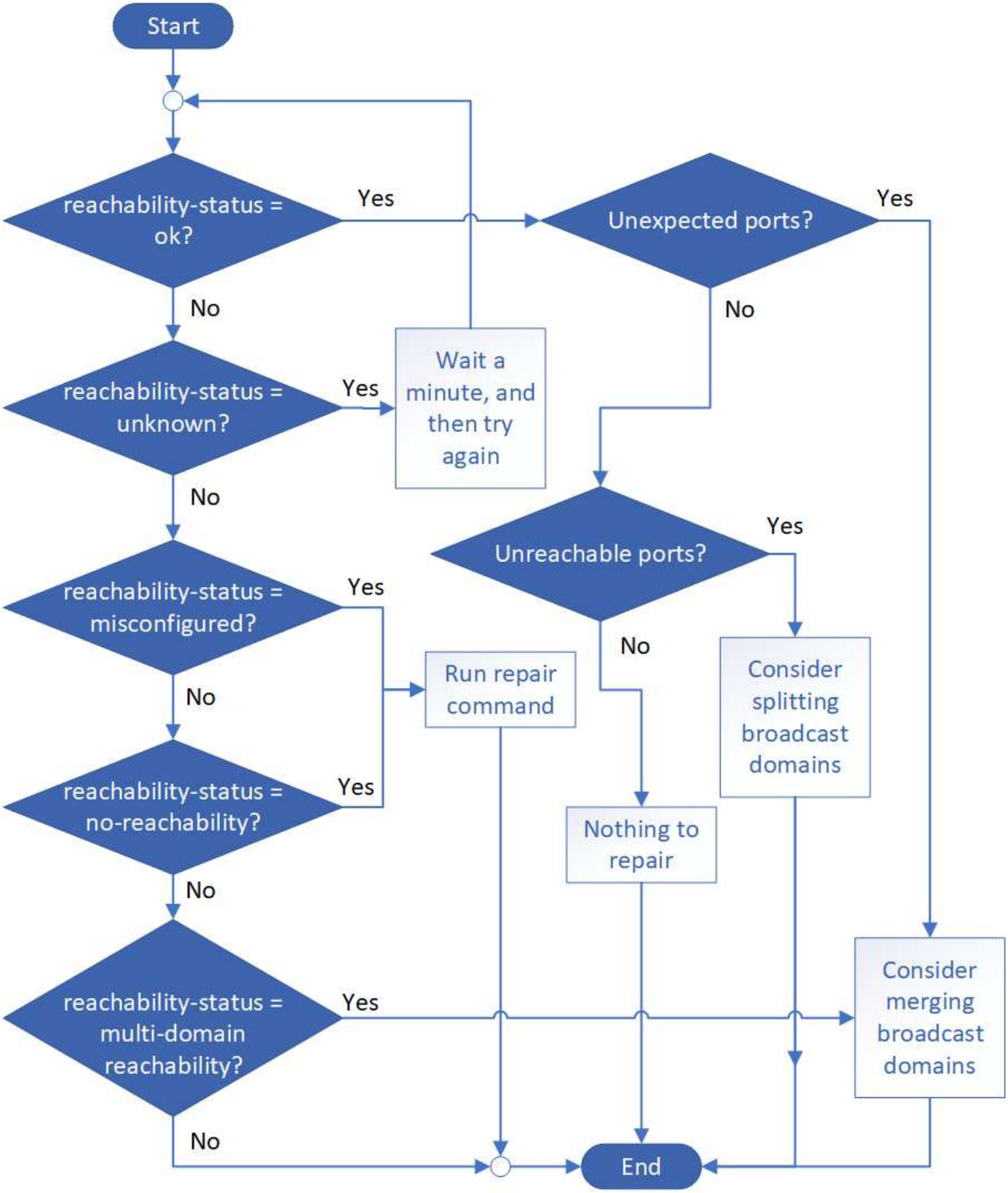
Verwenden Sie diese Befehle, um Fehlkonfigurationen in Netzwerken zu überprüfen, zu diagnostizieren und zu reparieren, die aus der ONTAP Konfiguration stammen und weder mit der physischen Verkabelung noch mit der Netzwerk-Switch-Konfiguration übereinstimmen.

Schritt

1. Port-Erreichbarkeit anzeigen:

```
network port reachability show
```

2. Verwenden Sie die folgende Entscheidungsstruktur und die folgende Tabelle, um den nächsten Schritt zu bestimmen, falls vorhanden.



Erreichbarkeit-Status	Beschreibung

ok	Der Port verfügt über eine Layer 2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne. Wenn der Status der Erreichbarkeit „ok“ ist, aber es „unerwartete Ports“ gibt, sollten Sie eine oder mehrere Broadcast-Domänen zusammenführen. Weitere Informationen finden Sie in der folgenden Zeile „*Unexpected Ports*“. Wenn der Status „Erreichbarkeit“ „ok“ lautet, aber „nicht erreichbare Ports“ vorhanden sind, sollten Sie eine oder mehrere Broadcast-Domänen aufteilen. Weitere Informationen finden Sie in der folgenden Zeile *Unerreichbare Ports*. Wenn der Status „Erreichbarkeit“ „ok“ lautet und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist die Konfiguration korrekt.
Unerwartete Ports	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Überprüfen Sie die physische Konnektivität und die Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domain des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen".
Nicht erreichbare Ports	Wenn eine einzelne Broadcast-Domäne in zwei unterschiedliche Wiederachabilität-Sets partitioniert wurde, können Sie eine Broadcast-Domäne teilen, um die ONTAP-Konfiguration mit der physischen Netzwerktopologie zu synchronisieren. In der Regel definiert die Liste der nicht erreichbaren Ports den Satz von Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollten, nachdem Sie überprüft haben, dass die physische und die Switch-Konfiguration korrekt ist. Weitere Informationen finden Sie unter "Teilen von Broadcast-Domänen auf".
Falsch konfigurierte Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit seiner zugewiesenen Broadcast-Domäne; der Port besitzt jedoch Layer 2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port der Broadcast-Domäne zu, der sie nachzuweisen kann: `network port reachability repair -node -port`Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".
Keine Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit für eine vorhandene Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port einer neuen automatisch erstellten Broadcast-Domäne im Standard-IPspace zu: `network port reachability repair -node -port`Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".

Multi-Domain-Erreichbarkeit	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Überprüfen Sie die physische Konnektivität und die Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domain des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen" Oder "Port-Erreichbarkeit reparieren".
Unbekannt	Wenn der Status „unbekannt“ lautet, warten Sie einige Minuten, und versuchen Sie den Befehl erneut.

Nachdem Sie einen Port repariert haben, müssen Sie die vertriebenen LIFs und VLANs überprüfen und beheben. Wenn der Port Teil einer Schnittstellengruppe war, müssen Sie auch verstehen, was mit dieser Schnittstellengruppe passiert ist. Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".

Übersicht über ONTAP-Ports

Eine Reihe bekannter Ports sind für die ONTAP-Kommunikation mit bestimmten Diensten reserviert. Port-Konflikte werden auftreten, wenn ein Port-Wert in Ihrer Speichernetzwerk-Umgebung mit dem des ONTAP Ports identisch ist.

In der folgenden Tabelle sind die von ONTAP verwendeten TCP-Ports und UDP-Ports aufgeführt.

Service	Port/Protokoll	Beschreibung
ssh	22/TCP	Sichere Shell-Anmeldung
telnet	23/TCP	Remote-Anmeldung
DNS	53/TCP	Lastverteilung des DNS
http	80/TCP	Hyper Text Transfer Protocol
Rpcbind	111/TCP	Remote-Prozeduraufruf
Rpcbind	111/UDP	Remote-Prozeduraufruf
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC
netbios-ssn	139/TCP	Sitzung für den NETBIOS-Dienst
snmp	161/UDP	Einfaches Netzwerkverwaltungsprotokoll
https	443/TCP	HTTP über TLS
microsoft-ds	445/TCP	Microsoft-ds
Montieren	635/TCP	NFS-Mount
Montieren	635/UDP	NFS-Mount
Genannt	953/UDP	Name Daemon

nfs	2049/UDP	NFS Server-Daemon
nfs	2049/TCP	NFS Server-Daemon
nrv	2050/TCP	NetApp Remote Volume Protokoll
iscsi	3260/TCP	ISCSI-Zielport
Verriegelt	4045/TCP	NFS-Sperr-Daemon
Verriegelt	4045/UDP	NFS-Sperr-Daemon
NSM	4046/TCP	Netzwerkstatusüberwachung
NSM	4046/UDP	Netzwerkstatusüberwachung
Rquotad	4049/UDP	NFS rquotad-Protokoll
Krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	Multicast-DNS
HTTPS	5986/UDP	HTTPS-Port - Binärprotokoll anhören
https	8443/TCP	7MTT GUI-Tool über HTTPS
ndmp	10000/TCP	Network Data Management Protocol
Cluster-Peering	11104/TCP	Cluster-Peering, bidirektional
Cluster-Peering, bidirektional	11105/TCP	Cluster-Peering
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	Steueranschlüsse über sichere Buchsen akzeptieren
cifs Witness Port	40001/TCP	cifs Witness Port
tls	50000/TCP	Sicherheit der Datenübertragungsschicht
iscsi	65200/TCP	ISCSI-Port

Interne ONTAP-Ports

In der folgenden Tabelle sind die TCP-Ports und UDP-Ports aufgeführt, die intern von ONTAP verwendet werden. Diese Ports werden für die Intracluster-LIF-Kommunikation verwendet:

Port/Protokoll	Beschreibung
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC
904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC

911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC
925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
931	NetApp Cluster RPC
932	NetApp Cluster RPC
933	NetApp Cluster RPC
934	NetApp Cluster RPC
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC
967	NetApp Cluster RPC
982	NetApp Cluster RPC
983	NetApp Cluster RPC
5125	Alternate Control Port für Festplatte

5133	Alternate Control Port für Festplatte
5144	Alternate Control Port für Festplatte
65502	Umfang des Node SSH
65503	LIF-Freigabe
7810	NetApp Cluster RPC
7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC
7822	NetApp Cluster RPC
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
8023	Knotenumfang-TELNET
8514	RSH mit Node-Umfang
9877	KMIP-Client-Port (nur interner lokaler Host)