9 Aug 2023 - DNS Addendum

Friday, August 4, 2023 7:33 AM

DNS Addendum

DNS Addendum incorporates lessons from the field' learning, improving on DNS product group alerting. Using the health model where critical (red) = outage, and warning = problem, NOT outage, as well as incorporating other best practices making for efficient monitoring that self-heals, has automation to eliminate most situations, leaving alerts that require manual intervention. Additionally, the addendum incorporates custom groups to remove DNS workflow 'burden' for all the synthetic nslookups per zone (forward and reverse) that happen per minute. Lastly, the addendum removes noisy DNS alerts, reduces config churn, as well as synthetic workflows produced by DNS 2016+ SCOM packs.

DNS Addendum also is similar with custom groups (luckily NOT as many as PKI customizations pack!)

Pre-requisites

Windows DNS packs MUST be installed

ID: Microsoft.Windows.DNSServer.2016
DisplayName: Microsoft Windows Server 2016 and 1709+ DNS Monitoring
Download SCOM 2016,2019 MP for DNS monitoring on Windows Server 2016 and 1709 Plus from Official Microsoft Download Center https://www.microsoft.com/en-us/download/details.aspx?id=54524

ID: Microsoft.Windows.Server.AD.2016.Monitoring
DisplayName: Active Directory Domain Services for Microsoft Windows Server 2016 and above (Monitoring)
Download Microsoft System Center Management Pack for ADDS from Official Microsoft Download Center
https://www.microsoft.com/en-us/download/details.aspx?id=54525

Windows DNS addendum downloaded and installed.

Create "Closed Alerts" view

To create a closed alert view in SCOM, follow these steps:

Open the Operations Console and navigate to the Monitoring workspace.

Click on the "New" button in the toolbar and select "Alert View" from the dropdown menu.
In the "Create Alert View" wizard, give your view a name and select "Closed Alerts" as the criteria.
Click "Next" and select the columns you want to display in your view.
Click "Next" again and choose any grouping or sorting options you want to apply.
Click "Finish" to create your view.
Once you have created your closed alert view, you can access it from the Alert Views folder in the Monitoring workspace. You can also customize the view further by right-clicking on it and selecting "Properties". From there, you can add or remove columns, change the grouping or sorting, and apply filters to further refine the view.

Configure Windows DNS Addendum for environment

Configure DNS Addendum for environment

Import DNS Addendum, if not already

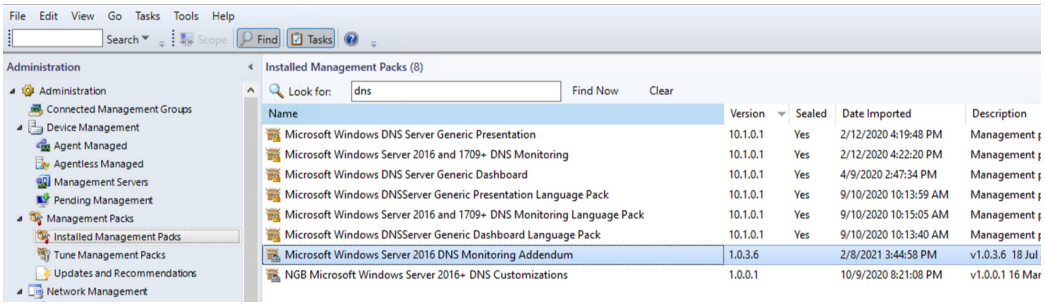
If DNS packs are NOT installed, wait 24 hours for discoveries to run and monitors and rules to begin alerting.
If DNS packs are installed, proceed to next step to verify two (2) overload monitors

To begin:

Copy file(s) to SCOM MS for import

Navigation steps:

Open SCOM Console
From Administration Tab > expand Management Packs folder > click on Installed Management packs
Click Import in the tasks pane on the right
Browse to file path > select the file > click Import
Proceed to next section



Verify DNS Query Overload monitors

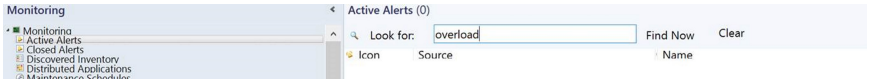
Simple find/replace can be done in Notepad++ (xml editor of preference) to update monitors for environment
Compare to actual values from environment, and any relevant alerts

Verify overload alerts
Use alert values to assess peaks to then update overrides in DNS Addendum

Navigation steps:
From SCOM Console > Monitoring Tab > Active Alerts

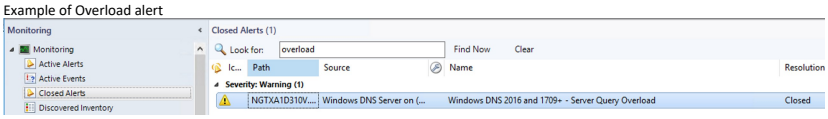
- In the 'Look for:' bar, type overload (and hit enter to search)

No 'Active alerts' is a good thing!
That means the addendum's default values are not causing alerts!



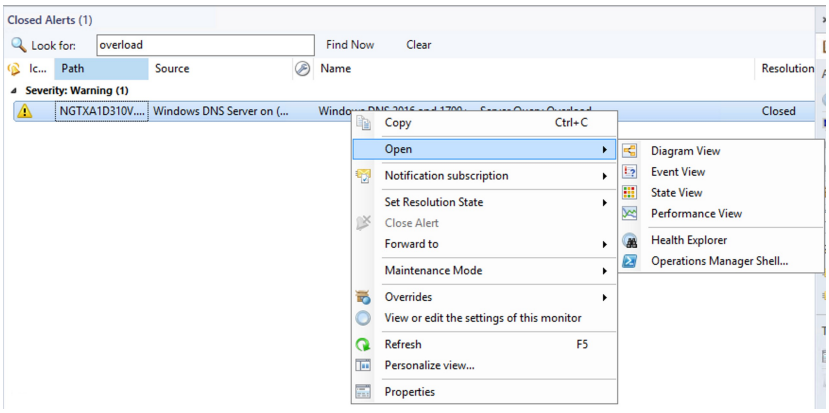
From SCOM Console > Monitoring Tab > Closed Alerts
Click on Closed Alerts
See pre-requisites steps to create view if NOT already there
In the 'Look for:' bar, type overload (and hit enter to search)

Example of Overload alert

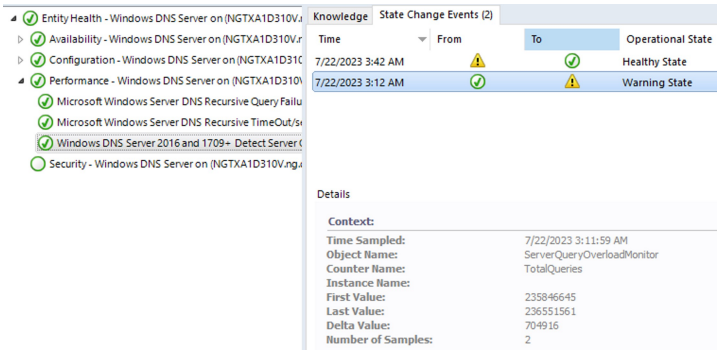


No 'alerts' is a good thing!
That means the addendum's default values have NOT caused alerts!

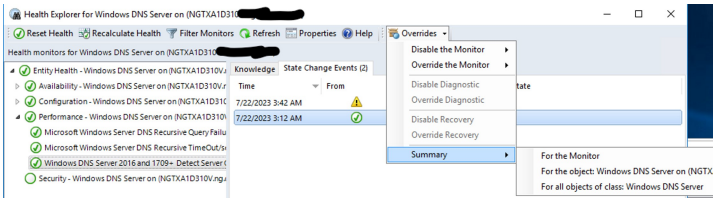
If alert exists, highlight alert
Right click (alternate mouse button) > Click on Open > Click on Health Explorer



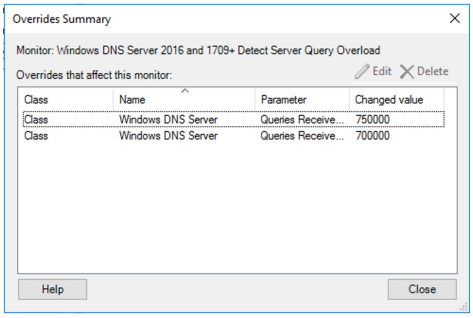
Click on Filter Monitors at the top
Expand Performance dropdown
Click on Detect Server
Click on the State Change Events, select the warning or critical state to see observed value



If the warning or critical value is way too (high/low), click on Overrides > Summary > For the Monitor

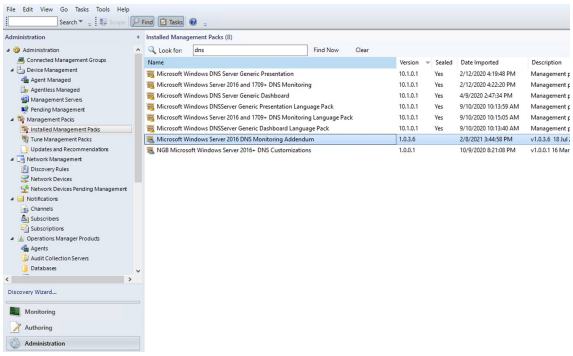


Edit values (warning/Critical)
Click Close

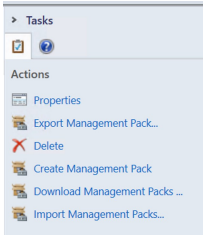


If changes made in GUI, backup pack to disk (i.e. Export Management Packs)

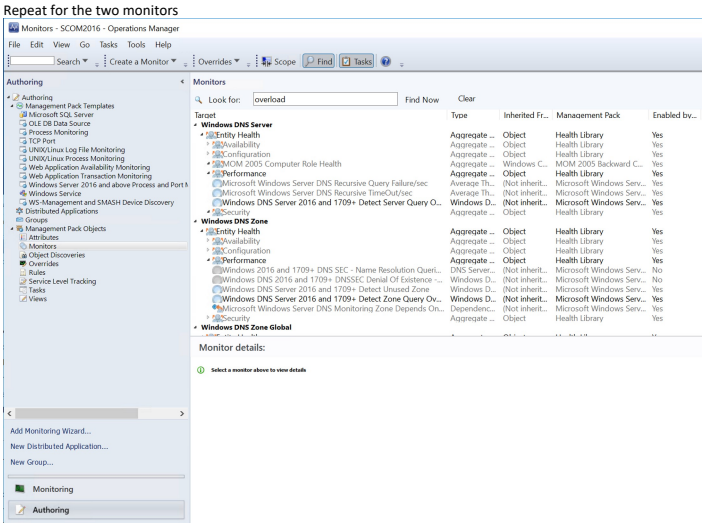
Navigation steps:
Click on Administration Tab > expand Management Packs folder > click Installed Management packs
Search for 'DNS Monitoring Addendum > highlight pack



Click Export Management Pack
Browse to file path > select the file > click Export
Proceed to next section to name non-system disk path to save file

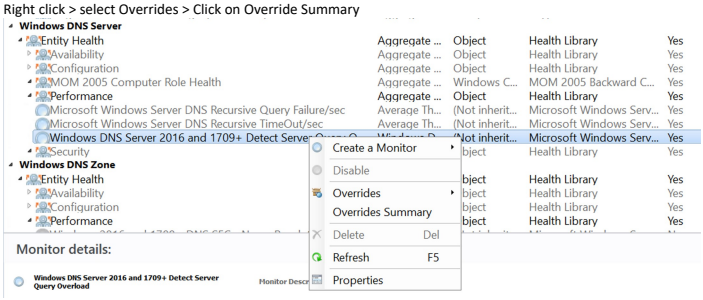


Steps for updating monitors from Authoring Tab
Alternate directions from SCOM Console > Authoring tab
Expand Management Pack Objects > click on Monitors
In the 'Look for:' bar, type overload
Repeat for the two monitors

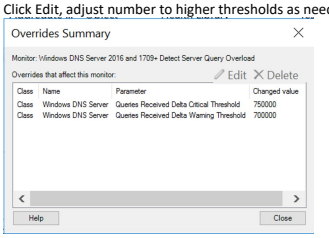


Begin with the 'Detect Server Query Overload' monitor

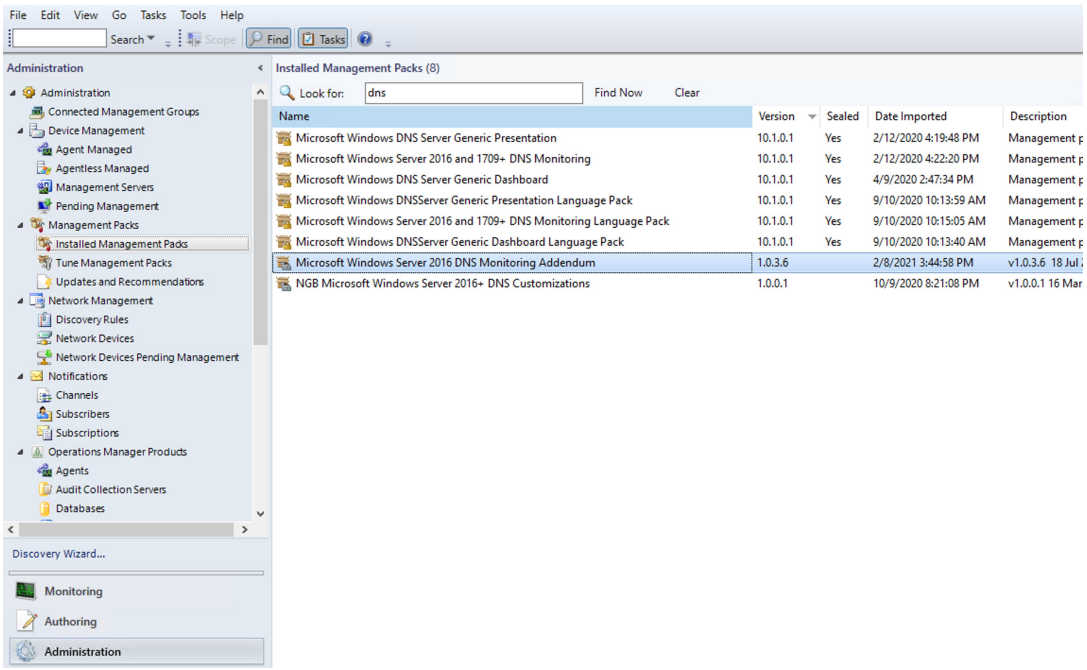
Right click > select Overrides > Click on Override Summary



Highlight one line at a time
Click Edit, adjust number to higher thresholds as needed



Repeat for Zone overload monitor



XML editing DNS Addendum pack

IF overload monitors were updated in the SCOM Console GUI

Open the exported file and continue with XML edits in your favorite XML editor.

Update Synthetic monitor DS and WA

Proactive.DNSAlerts.Synthetic.Monitor.Datasource

Update Line 632 - Proactive.DNSAlerts.Synthetic.Monitor.Datasource

Adjust internal and external nslookups (

External nslookup = ESPN.com

Internal nslookup = $InternalDNS = "ocsp.##FQDN##"

Update Discoveries

Lines 1715-1872

Update naming convention for DC PDC emulator role server(s) with AD Integrated DNS servers

Efficient monitoring to reduce workflows running on DC

Update the Pattern Regular Expression (RegEx) to match your naming convention

Find ##PDCEmulatorRoleDCs## (Control-H) and Replace with naming convention(s)

Example Discovery with multiple naming conventions in discovery

```
<Discoveries>
  <Discovery ID="Windows.DNS.Root.Domain.Controllers.Group.DiscoveryRule" Enabled="true" Target="Windows.DNS.Root.Domain.Controllers.Group" ConfirmDelivery="false" Remotable="t
    <Category>Discovery</Category>
    <DiscoveryTypes>
      <DiscoveryRelationship TypeID="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities" />
    </DiscoveryTypes>
    <DataSource ID="GroupPopulationDataSource" TypeID="SC!Microsoft.SystemCenter.GroupPopulator">
      <RuleId>$MPElement$</RuleId>
      <GroupInstanceId>$MPElement[Name="Windows.DNS.Root.Domain.Controllers.Group"]$</GroupInstanceId>
      <MembershipRules>
        <MembershipRule>
          <MonitoringClass>$MPElement[Name="MWD2!Microsoft.Windows.DNSServer.2016.Server"]$</MonitoringClass>
          <RelationshipClass>$MPElement[Name="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities"]$</RelationshipClass>
          <Expression>
            <RegExExpression>
              <ValueExpression>
                <HostProperty>
                  <MonitoringClass>$MPElement[Name="Windows!Microsoft.Windows.Computer"]$</MonitoringClass>
                  <Property>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Property>
                </HostProperty>
              </ValueExpression>
              <Operator>MatchesRegularExpression</Operator>
              <Pattern>(?i)A1|nge[ew]a1d3..p.ngman|cc0</Pattern>
            </RegExExpression>
          </Expression>
        </MembershipRule>
      </MembershipRules>
    </DataSource>
  </Discovery>
```

Repeat for the other groups (list below)

- Windows DNS - PDC Emulator role Domain Controllers
- Windows DNS Server IP Address - PDC Emulator role domain controllers
- Windows DNS Forwarder Conditional Forward - PDC Emulator role domain controllers
- Windows DNS Zone - PDC Emulator role Domain Controllers

Enable Synthetic DNS monitor

This is disabled by default, as it's optional content and functionality.
Basically the monitor is a PowerShell script running two nslookups, where failure creates alert

```
    <UnitMonitor ID="Proactive.DNSAlerts.Synthetic.Monitor" Accessibility="Public" Enabled="false" Target="MWD2!Microsoft.Windows.DNSServer.2016.Server" ParentMonitorID="Health!S
  </Monitors>
```

Update Group overrides

Verify GUID(s) are not in use for overrides

Lines 3388 - 3620

From PowerShell get the object GUID

```
get-scomclassinstance -ID "95dc6ec7-234f-00fc-5851-ae49eb5d8531"
get-scomclassinstance -ID "31516f6c-e158-259f-9525-b46559698bfd"
get-scomclassinstance -ID "1c71d791-20ba-4157-0f6d-9d4ad52040f7"
```

Groups that DNS Addendum pack adds:

- Windows DNS - PDC Emulator role Domain Controllers
- Windows DNS Server IP Address - PDC Emulator role domain controllers
- Windows DNS Forwarder Conditional Forward - PDC Emulator role domain controllers
- Windows DNS Zone - NGMAN Domain Controllers

If Addendum pack is already installed, check the group(s) to find the GUIDs

```
get-scomclassinstance -DisplayName "Windows DNS - PDC Emulator role Domain Controllers" | ft
Id
get-scomclassinstance -DisplayName "Windows DNS Server IP Address - NGMAN domain
controllers
get-scomclassinstance -DisplayName "Windows DNS Forwarder Conditional Forward - NGMAN
domain controllers" | ft Id
get-scomclassinstance -DisplayName "Windows DNS Zone - PDC Emulator role Domain
Controllers" | ft Id
```

Use the values from the above commands to replace the 'ContextInstance' values in the Overrides section

Action: Find the GUIDs, then create the get-SCOMClassInstance syntax

```
<Overrides>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Server.Property.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Discov
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Server.Property.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95d
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.TrustPoint.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Discovery="
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.TrustPoint.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95dc6ec7
    <Value>false</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Forwarder.Conditional.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false"
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Forwarder.Conditional.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstanc
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.ClientSubnet.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Discovery
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.ClientSubnet.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95dc6e
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.RecursionScope.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Discove
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.RecursionScope.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95dc
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Policy.ServerLevel.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Dis
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Policy.ServerLevel.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.ZoneScope.Discovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Zone" Enforced="false" Discovery="MWD
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.ZoneScope.Discovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95dc6ec7-
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Zone.0to10PercentDiscovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Disco
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Zone.0to10PercentDiscovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="95
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Zone.70to80PercentDiscovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Disc
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Zone.70to80PercentDiscovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="9
    <Value>true</Value>
  </DiscoveryPropertyOverride>
  <DiscoveryPropertyOverride ID="Override.Microsoft.Windows.DNSServer.2016.Zone.20to30PercentDiscovery" Context="MWD2!Microsoft.Windows.DNSServer.2016.Server" Enforced="false" Disc
  <DiscoveryPropertyOverride ID="Override.Group.Microsoft.Windows.DNSServer.2016.Zone.20to30PercentDiscovery" Context="Windows.DNS.Root.Domain.Controllers.Group" ContextInstance="9
```

Find/replace the GUIDs from the commands above to update the DNS Addendum pack

Version Pack
Change the version to help Configuration service (cshost) to know management pack changed

Update line 5, from 1.0.3.6 to 1.0.3.7

```
1   <?xml version="1.0" encoding="utf-8"?><ManagementPack ContentReadable="true"
2     <Manifest>
3       <Identity>
4         <ID>Microsoft.Windows.Server.DNS.Monitoring.Addendum</ID>
5         <Version>1.0.3.6</Version>
6       </Identity>
7       <Name>Microsoft Windows Server 2016 DNS Monitoring Addendum</Name>
8       <References>
50    </Manifest>
```

Find/Replace the PowerShell workflows

Find	.v1037.ps1
Replace	.v1037.ps1

Add change log entry in Description for new version

```
3650    <LanguagePacks>
3651      <LanguagePack ID="ENU" IsDefault="false">
3652        <DisplayStrings>
3653          <DisplayString ElementID="Microsoft.Windows.Server.DNS.Monitoring.Addendum">
3654            <Name>Microsoft Windows Server 2016 DNS Monitoring Addendum</Name>
3655            <Description>
3656  v1.0.3.6  18 Jul 2023 - Updated alert severity
3657  v1.0.3.5  27 Jun 2023 - ADI DNS count monitors for 3152,7616
3658  v1.0.3.4  13 Jun 2023 - Additional overrides to disable rules, added count logic monitors on DNS events, reports to informational
3659  v1.0.3.3   9 Jun 2023 - WA for nslookups, Recovery task for WMI validations, Query overload value changes CRIT/WARN
3660  v1.0.3.3  31 Jan 2023 - Added ADI 404,408 count monitors, DNS internal/external powershell monitor
3661  v1.0.3.2  23 Jan 2023 - Updated Cleanup methods with get modules, ADI count monitors
3662  v1.0.2.9   5 Jan 2023 - ADI and DNS Server logging alerts set to warning
3663  v1.0.2.7  15 Jul 2022 - MonitorTypes, Recovery Automation
3664  v1.0.2.2  14 Jun 2022 - Updated run times
3665  v1.0.1.5  18 Mar 2022 - Updated overrides to disable except for root DNS servers, additional logic
3666  v1.0.1.4   8 Dec 2021 - Updated Proactive.DailyTasks.DNSAlerts.Report.Script.Alert.Rule to 1200
3667  v1.0.0.11 18 Mar 2021 - Updated Tasks, script versions
3668  v1.0.1.1  11 May 2021 - Updated Report datasource, moving report to front, updated monitors/alerts
3669  v1.0.0.13 26 Mar 2021 - Added 'Windows DNS - Active Directory Integrated Write Failed' to autoclose rules
3670  v1.0.0.9  16 Mar 2021 - Updated Daily Summary and autoclose reports
3671  v1.0.0.6  10 Mar 2021 - Added DailySummary datasource, task, rules, alerts
3672  v1.0.0.3   9 Mar 2021 - Updated property, delivered pack with daily report/task, recovery automation for EventID 4015
3673  v1.0.0.0   8 Feb 2021 - Created for DNS server alert tuning</Description>
```

Save file
Import to SCOM