Exchange Server 2016
Tipy & triky

Miroslav Knotek
MVP: Cloud and Datacenter Management, MCSE: messaging
IT konzultant – KPCS CZ, s.r.o.
knotek@kpcs.cz
Agenda

- Aktuality ze světa Exchange Server 2016
- Tipy a triky pro
  - Nasazení
  - Optimalizaci
  - Provoz
Exchange 2016 Servicing Model

- Exchange 2016 continues the Cumulative Update model
- CUs are shipped quarterly and critical updates (e.g. security updates) will be released as needed on “patch Tuesday.”
- Service packs will not be shipped for Exchange 2016.
- Only versions CUn and CUn-1 will be serviced for product fixes.
- Customers with hybrid relationships to O365 are required to be on one of the two most recent updates for their major Exchange version, be it 2010, 2013, or 2016 as of today.
- Application bits are now distributed in ISO format.
  - Yes, you can mount/extract to a network share and then install.
Server requirements

- Exchange 2016 is supported on full GUI installs of
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016 (RTM only, no pre-release builds. Requires CU3 or later.)

- Exchange 2016 requires
  - .NET Framework 4.5.2 or 4.6.x (More on that later!)
  - Windows Management Framework 4.0
  - Unified Communications Managed API (UCMA) 4.0
Exchange and Windows Server 2016

- You cannot upgrade OS on a server with Exchange installed
- You cannot use /RecoverServer to change the OS on a server with Exchange installed
- New installs are the only way to take advantage of Windows Server 2016
- Windows Defender is on by default in Windows Server 2016
  - We recommend the Exchange installation and setup log folders be excluded from scanning in Windows Defender
  - We also recommend excluding noderunner.exe processes from scanning
Server 2016 High Availability Enhancements

- **Storage Replica**
  - Similar to Hyper-V Replica, unsupported at this time
  - Block-based replication may not always align with Exchange transaction-based databases

- **VM Storage Resiliency**
  - No official support statement yet
  - Recommend disabling it for Exchange virtualized DAGs (let Exchange determine when to failover)

- **Production Checkpoints**
  - Same story as before, not supported at this time
  - Exchange config shared between AD & Exchange Server, Checkpoints problematic in production
.NET 4.6.1 and 4.6.2 (For Exchange 2013 CU13/Exchange 2016 CU2 or later)

- .NET 4.6.1 supported if the following hotfixes are installed
  - Windows Server 2008 / 2008 R2
    https://support.microsoft.com/kb/3146716
  - Windows Server 2012
    https://support.microsoft.com/kb/3146714
  - Windows Server 2012 R2
    https://support.microsoft.com/kb/3146715

- .NET 4.6.2 to become supported with 2013 CU15 and 2016 CU4.
  - No additional hotfixes required with 4.6.2

- .NET 4.6.2 to become mandatory with 2013 CU16 and 2016 CU5.
  - Setup will block installation if 4.6.2 is not detected
Windows Management Framework

What should we expect to see?

- Did the OS ship with it? It is supported.

  e.g. *Windows Server 2016 ships with WMF5, therefore Exchange 2016 CU3 or later can use WMF5 if installed on Windows Server 2016, but not if installed on Windows Server 2012 R2 as that OS did not ship with WMF5.*

- Do you have to install it to use it? Then it is not supported.
Exchange Supportability Matrix

http://aka.ms/essm
DAG Activation Preference Behavior Change

- **Introduced in 2016 CU2**
  - All servers within DAG need to be CU2
  - If upgrading, feature takes effect after last node is updated
- Automatically redistributes using Activation Preference if a lossless activation is possible
  - Replaces RedistributeActiveDatabases.ps1 script
  - Can remove any scheduled tasks after upgrading to CU2
- Can control frequency of moves
  - `Set-DatabaseAvailabilityGroup <Name> -PreferenceMoveFrequency <value in the format of 00:00:00>`
  - Default value is one hour 01:00:00
  - To disable feature: `Set-DatabaseAvailabilityGroup <Name> -PreferenceMoveFrequency ([System.Threading.Timeout]::InfiniteTimeSpan)`
Read from Passive

- **Introduced in 2016 CU3**
- Allows Content Indexes to be built from local passive copy
- Previously required traversing network to read from active copy to create Content Index
- Significant potential bandwidth savings
  - Content Indexing can generate as much network traffic as replication log shipping!
Potential savings

Example: If DB1 generates 5GB of transaction logs a day and has 4 copies (1 Active/3 Passive), then how much data traverses the network per day for these copies?

- 3 Replication streams
- 3 * 5GB = 15GB

Now what about Content Indexing bandwidth?

In the above scenario (before CU3):

- Replication Traffic = 15GB
- Content Index Traffic = 15GB (CI Traffic = 1X Uncompressed Replication Traffic)
- Total Traffic = 30GB

With CU3 and Read from Passive:

- Replication Traffic = 15GB
- Content Index Traffic = 0
- Total Traffic = 15GB

Note: For Lagged Copies, CI traffic must still connect to Active Copy and therefore traverse network
Read from Passive: As seen in calculator

### Exchange 2013

<table>
<thead>
<tr>
<th>Description</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Log &amp; Content Index Throughput Required / Database</td>
<td>1.33 Mbps</td>
</tr>
<tr>
<td>Peak Log &amp; Content Index Throughput Required Between Datacenters / DAG</td>
<td>3.3581 Mbps</td>
</tr>
<tr>
<td>Total Peak Log &amp; Content Index Replication Throughput Required / Environment</td>
<td>3.3581 Mbps</td>
</tr>
</tbody>
</table>

### Exchange 2016 with CU3 (30% Reduction)

<table>
<thead>
<tr>
<th>Description</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Log &amp; Content Index Throughput Required / HA Database Copy</td>
<td>0.55 Mbps</td>
</tr>
<tr>
<td>Peak Log &amp; Content Index Throughput Required / Lagged Database Copy</td>
<td>1.33 Mbps</td>
</tr>
<tr>
<td>Peak Log &amp; Content Index Throughput Required Between Datacenters / DAG</td>
<td>2.3704 Mbps</td>
</tr>
<tr>
<td>Total Peak Log &amp; Content Index Replication Throughput Required Between Datacenters</td>
<td>2.3704 Mbps</td>
</tr>
</tbody>
</table>
Deprecation of SmartScreen

SmartScreen spam filters in Outlook and Exchange are obsolete and have been replaced by Exchange Online Protection (EOP), a more effective, cloud-based email filtering service.

On November 1, 2016, Microsoft will stop generating updates for the SmartScreen spam filters for:
- Outlook 2011 for Mac

SmartScreen spam filter will be removed from future versions of Exchange Server and Outlook for Windows.

No changes to the SmartScreen Filter online protection features built into Windows, Microsoft Edge and Internet Explorer.
Best practices and tips
Deployment
Tip: a few useful PowerShell scripts for Exchange and Office 365 Admins

Generate Antivirus Exclusions for Exchange 2013 and 2016 Servers

These PowerShell scripts generate a list of file, folder, process file extension exclusions for configuring antivirus software that will be running on an Exchange 2013 or Exchange 2016 servers.

Use the scripts to generate the exclusion list based on a single server. You can then apply the same exclusions to all servers that have the same configuration.

The scripts are based on information published by Microsoft:
- [Exchange Server 2013 antivirus exclusions](https://gallery.technet.microsoft.com/office/Generate-Antivirus-f1a9a59e)
- [Exchange Server 2016 antivirus exclusions](https://gallery.technet.microsoft.com/office/Generate-Antivirus-f1a9a59e)
- `ConfigureWindowsDefender` switch that will add the exclusions to Windows Defender on the local server.

Download script from https://gallery.technet.microsoft.com/office/Generate-Antivirus-f1a9a59e
Demo: Set-Exchange2016Prerequisites-1.7.ps1 & ExchangeServerAntivirusExclusions.ps1
Server requirements

Optional Requirements

- Office Online Server *(Bits available only via Volume License Service Center)*
  - Provides OWA the ability to preview attachments
  - No long using 3\textsuperscript{rd} party licensed software to do previewing

- SharePoint 2016
  - Provides the ability to use “cloudy attachments”
  - Send a link to a OD4B doc instead of a full file attachment.
Office Online Server and OOtW

* = Internal DNS Only
Demo: Deployment of Office Online Server (OOS)
Before Attachment Viewing is Configured

That’s all folks!

No Native App Installed

Native App Installed
Configuring Attachment Viewing

Configure the WAC discovery endpoint per mailbox server

```bash
[PS] C:\>Get-MailboxServer E16LAB-2K16-101 | FL WACDiscovery*
WACDiscoveryEndpoint :

[PS] C:\>Get-MailboxServer E16LAB-E2K16-101 | FL WACDisc*
WACDiscoveryEndpoint : https://oos.us.corp.e16lab.com/hosting/discovery
```

Restart MSExchangeOWAAppPool

If you are missing WACDiscoveryEndpoint on Set-MailboxServer, run Setup /PrepareAd to update RBAC.
After Attachment Viewing is Configured

Look, Mom, two options now!

The new side-by-side (SxS) view
For On-Premises Cloudy Attachments you’ll need:

1. OOS setup and working with Exchange
2. SharePoint 2016 configured for MySites
3. SharePoint WOPI Binding established with OOS via New-SPWOPIBinding
4. OAuth configured on SP to trust EX (Script available soon)
5. OAuth configured on EX to trust SP (Script shipped with Exchange)
6. Configure OWA Mailbox Policy InternalSPMySiteHostURL and ExternalSPMySiteHostURL values and policy assigned to users.
   • Or the OWA vDirs themselves if you need server-level granularity.
Client Access Service and Kerberos Authentication

The Problem

- Kerberos authentication is not enabled by default

Why?

- Client negotiates Kerberos Authentication
- Client obtains Kerberos service tickets in the context of the load-balanced Client Access services
- Client submits tickets to CAS member
- CAS member runs within its local context and thus has a context mismatch which results in Kerberos authentication failure

- SPN’s must be unique in a domain and so multiple CAS can’t have the same SPN, required for Kerberos to work
CAS Arrays and Kerberos Authentication
The Solution

- In order to utilize Kerberos authentication, there must be a shared credential that can be used by all CAS members

Steps

- Create an account (machine account is preferred) with minimal rights
- Distribute this account to each CAS member using the RollAlternateServiceAccountCredential.ps1 script which applies the credentials to each CAS as well as, configures password settings for the account
  - Remember to do this on CAS members in the secondary datacenter!
- Register all the SPNs to the account
  - Setspn –a http/<CAS FQDN> <kerbserviceaccount>
- Configure Outlook Anywhere and MAPI over HTTP for negotiate authentication
- Restart Outlook
Demo: Configuring Kerberos authentication
Witness Server Placement

New Witness Server placement options available
- Choose based on business needs and available options

Third location DAG witness server improves DAG recovery behaviors
- Automatic recovery on datacenter loss
- Third location network infrastructure must have independent failure modes

<table>
<thead>
<tr>
<th>Deployment scenario</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAG(s) deployed in a single datacenter</td>
<td>Locate witness server in the same datacenter as DAG members; can share one server across DAGs</td>
</tr>
<tr>
<td>DAG(s) deployed across two datacenters; No additional locations available</td>
<td>Locate witness server in primary datacenter; can share one server across DAGs</td>
</tr>
<tr>
<td>DAG(s) deployed across two+ datacenters</td>
<td>Locate witness server in third location; can share one server across DAGs</td>
</tr>
</tbody>
</table>
Azure-hosted Witness Server

- Domain controllers replicated from on-premises must be deployed in Azure
- Domain name resolution configured between Windows Azure and on-premises
  - Typically provided by domain controllers deployed in Windows Azure
Multiple Databases Per Volume

What’s the benefit?
- Better use of large capacity drives (8TB)
- Max recommended database size is still 2TB
- Faster reseed times with AutoReseed
- Seeding 4 1.5TB databases is faster than 1 6TB DB
- No longer source constrained
Use REFS

- ReFS is recommended for volumes containing Exchange database files, log files, and content index files.
- ReFS data integrity features are recommended to be disabled:
  - Format-Volume -FileSystem REFS -NewFileSystemLabel ExchLUN01 -SetIntegrityStreams $false
- Autoreseed the disk reclaimer needs to know which file system to use when formatting spare disks:
  - Set-DatabaseAvailabilityGroup DAG01 -FileSystem ReFS
- Be aware of compatibility:

```yaml
DPM overview
  - What's new in DPM
  - System requirements
DPM protection support matrix
  - Supported and unsupported
```


- On-premises Hyper-V virtual machine
- From DPM 2012 R2 Update Rollup 9 onwards
  - Only supported if the Exchange database is on NTFS. REFS isn't currently supported.
- VMware Windows VM
Cache is King

A storage controller with protected cache is a must
In most storage solutions, this implies using RAID controller (JBOD controller is usually just a pass-through HBA without any cache)
Present each physical disk as a separate single disk RAID-0 virtual disk; use 256KB stripe size
Make sure controller cache is flash or battery protected
Enable caching policy with 100% write cache
Do not use cache on physical disk itself as it is not protected
Beware pinned/preserved cache!

Without write cache, disk write performance is dramatically impaired
Jetstress 2013 on HGST He6 7200rpm 3.5” disks with LSI SAS 9380-8e: ~90 IOPS/disk with write caching enabled!
Jetstress 2013 on the same disks and controller but without cache: 3-4 IOPS/disk (Yes, 3-4!!!)
before log write latency exceeds 10ms

We will still support you but the pain will be all yours... ;)

Scale-up? Scale-out? Scale to 5th dimension?

**Server-level**
- Recommendations to scale no greater than 24 CPU cores and 96GB of RAM
- Based on best performance and stability seen in Office 365
- Have been support incidents where performance impacted at large-scale
- Guidance now in Exchange Server Role Requirements Calculator

**DAG-level**
- Recommendation: Build your DAG out to 16 nodes before creating new DAGs
- Larger DAGs, combined with Dynamic Quorum can increase availability in failure scenarios
- Larger DAG=Better Resiliency
Before Dynamic Quorum
With Dynamic Quorum
Exchange 2013/2016 Message Tracking Log GUI


![Message Tracking Log GUI](https://gallery.technet.microsoft.com/office/Exchange-2013-Message-875b3eeb)

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Sender</th>
<th>Recipients</th>
<th>Message Subject</th>
<th>EventId</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/10/2015 12:02:15 AM</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>RECEIVE</td>
<td></td>
</tr>
<tr>
<td>12/10/2015 12:02:15 AM</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>DELIVER</td>
<td></td>
</tr>
<tr>
<td>12/10/2015 12:02:15 AM</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>SEND</td>
<td></td>
</tr>
<tr>
<td>12/10/2015 12:02:15 AM</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>DELIVER</td>
<td></td>
</tr>
<tr>
<td>12/10/2015 12:02:15 AM</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>[Success] Backup Exec Alert Job Success</td>
<td>SEND</td>
<td></td>
</tr>
</tbody>
</table>
Demo: Message Tracking GUI
Turn off access to the Exchange admin center

By default, access to the EAC isn't restricted, and access to Outlook on the web on an on an Internet-facing Exchange server also gives access to the EAC. Organizations may want to restrict access to the EAC for client connections from the Internet.

You can set the AdminEnabled parameter to the value $false on the EAC virtual directory but you disable access to the EAC for internal and external client connections.

If you want restrict access from the Internet, follow the guideline https://technet.microsoft.com/en-us/library/jj218639(v=exchg.160).aspx

- Set-ECPVirtualDirectory -Identity "<Server>\ecp (Default Web Site)" -AdminEnabled $false

2 options supported

- Configure a second Exchange 2016 server that's only accessible from the internal network to handle internal EAC connections.
- On the existing Exchange 2016, create a new IIS web site with new virtual directories for the EAC and Outlook on the web that's only accessible from the internal network.
Export/Import PST

- Available only in the Mailbox Import Export role, and by default, that role isn't assigned to a role group
  - you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group)
  - `New-ManagementRoleAssignment -Role "Mailbox Import Export" -User "<user name or alias>"`
- `New-MailboxExportRequest -Mailbox <user> -ContentFilter {((Received -lt '01/01/2013') -and (Subject -like 'fwd*'))} -FilePath \<server FQDN>\<shared folder name>\<PST name>.pst`
Performing maintenance on DAG members

- StartDagServerMaintenance.ps1/StopDagServerMaintenance.ps1 for Exchange 2010 only.

- Supported steps for performing maintenance on DAG members

- Exchange 2016 and Exchange 2013 Post-Patching or Restart Script

- Exchange 2016 and Exchange 2013 Pre-Patching or Restart Script